

Das Kriminalitätslagebild im Land Sachsen-Anhalt und der Beitrag des polizeilichen Beratungsangebotes für die Unternehmenssicherheit

Vortrag des Direktors des LKA, Frank Hüttemann,
am 13.09.2007 vor dem

Verband für Sicherheit in der Wirtschaft Mitteldeutschland e. V. (VSWM)

Landeskriminalamt Sachsen-Anhalt
Lübecker Str. 53 – 63
39124 Magdeburg
-Der Direktor-

Verfasser:

Frank Hüttemann
Hans-Joachim Wriedt
Gerd Engelke

Torsten Meyer
Norbert Heinrichs

Volkmar Hellwig
Tel.: 0391 – 250 0

Fax: 0391 – 250 193011

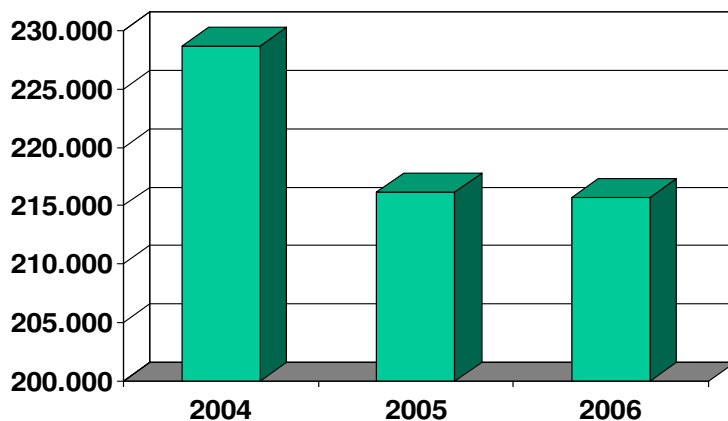
ag-kripo@lka.pol.sachsen-anhalt.de

I. Allgemeine Aspekte der Lageentwicklung

Meine Damen und Herren,

im ersten Teil meines Vortrages werde ich mich mit der Kriminalitätsentwicklung in Sachsen-Anhalt im Jahr 2006 befassen. Das ist, um es mit Günther Grass zu sagen, ein weites Feld und würde, bei ausführlicher Darstellung meinerseits den zeitlichen Rahmen dieser Veranstaltung sprengen. Ich werde mich bei meinen nachfolgenden Ausführungen deshalb auf ausgewählte Bereiche der Kriminalität beschränken, zumal auf solche, die direkt oder indirekt die Sicherheit von Unternehmen bedrohen.

Wenn von der Entwicklung der Kriminalität die Rede ist, kann es nicht ausbleiben, dass man



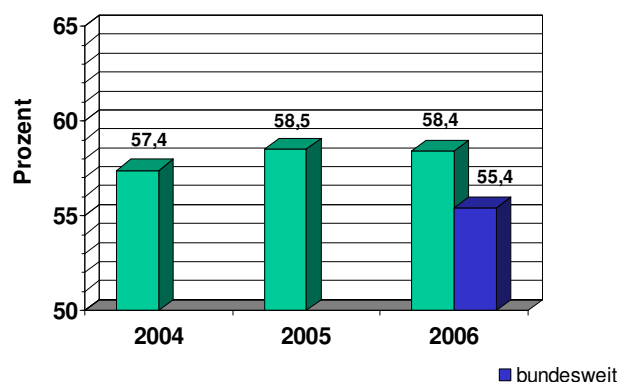
sich der Polizeilichen Kriminalstatistik, kurz PKS zuwendet. Diese weist für das Jahr **2006** in Sachsen-Anhalt **215.730** Delikte auf, **2005** waren es **216.186** und **2004 228.647**.

Es bleibt zu hoffen, dass der Rückgang der Kriminalität auch in der Zukunft weiter anhält.

Was das Fallaufkommen im Einzelnen anbetraf, so waren im Jahr 2006 allein **59,7 %** aller Delikte dem Diebstahl bzw. Vermögens- oder Fälschungsdelikten zuzuordnen. Der Anteil der Straftaten gegen das Leben betrug - auch wenn die Berichterstattung in den Medien häufig ein anderes Bild zeichnet - nur **0,1%**. Ein signifikanter Rückgang war bei Diebstahl, der Straßenkriminalität und bei den Raubdelikten zu verzeichnen.

Auch die Aufklärungsquote ist auf einem beständig hohen Niveau. **2006** lag sie **58,4%**, **2005** betrug sie **58,5%**, **2004** wies sie einen Wert von **57,4%** auf.

Zum Vergleich, bundesweit lag die Aufklärungsquote 2006 bei 55,4%.



Ist also alles in bester Ordnung? Gibt es keinen Grund zur Sorge? Oder muss man das Bild etwas differenzierter betrachten?

Im Jahre **2006** sind die **Wirtschaftsstrafaten** in Sachsen-Anhalt von **1578 Verfahren (2005) auf 2470 Vorgänge** angestiegen, dies ist eine Steigerung der Fallzahlen um **64,1%**.

Wirtschaftskriminalität	+ 64,1 %
Computerkriminalität	+ 10,01 %
Wettbewerbsdelikte	+ 181,8 %
Korruptionsdelikte	+ 788,5 %

Die Kriminalität unter Nutzung von Informations- und Kommunikationstechnologie (IuK Kriminalität) volkstümlich Computerkriminalität genannt, hat sich, was sie Zahlen anbelangt, von **1507 Delikten (2005) auf 1659 Delikte** erhöht, was eine Steigung der Fallzahlen von **10,01%** bedeutet. Die Anzahl der **Wettbewerbsdelikte**, hier sind vor allem die **Produkt- und Markenpiraterie** zu nennen erhöhte sich im Jahresvergleich **2005/2006** um **181,8%** (2005: 148 Fälle, 2006: 417). **Die Korruptionskriminalität** hat sich um **788,5%** erhöht (26 Fälle in 2005, 205 Fälle in 2006).

Diese wenigen Zahlen belegen, dass es trotz der unbestreitbar positiven Gesamtentwicklung Deliktsfelder gibt, die beträchtliche Steigerungsraten zu verzeichnen haben. Es kristallisiert sich auch immer mehr heraus, dass die Täter in den verschiedensten Deliktsbereichen immer häufiger zur Tatbegehung bzw. für Folgetaten das Tatmittel Internet nutzen (z. B. beim Warenbetrug, Urheberrechtsverletzungen etc.).

Im Folgenden möchte ich nun die von mir angesprochen Straftatengruppen näher beleuchten. Wir werden uns kurz mit der Phänomenologie dieser Delikte auseinandersetzen und der Frage nachgehen, inwieweit von diesen kriminellen Handlungen eine spezifische Bedrohungssituation für Unternehmen ausgeht. Zur Illustration möchte ich Ihnen dabei einige exemplarische Fälle aus Sachsen-Anhalt schildern. Der letzte Teil meiner Ausführungen wird sich mit der Frage befassen, welchen konkreten Beitrag die polizeilichen Beratungsstellen für die Sicherheit von Unternehmen leisten.

Bevor wir uns jedoch mit diesen Themen befassen, werden wir uns ein aktuelles Beispiel aus den Eigentumsdelikten ansehen, welches zumindest für eine Gruppe von Unternehmern auch von nicht geringer Bedeutung sein dürfte, die Diebstähle von Baumaschinen und Fahrzeugen.

Auch wenn Täter heute vermehrt im Anschluss oder zur Begehung von Taten das Internet nutzen, sollte man nicht aus den Augen verlieren, dass Unternehmen in ihrer Mehrzahl durch

Delikte herkömmlicher Art beeinträchtigt werden, Eigentums- und Vermögensdelikte spielen dabei die größte Rolle.

II. Diebstähle von Baumaschinen und Baufahrzeugen

Ein Beispiel dafür sind die Diebstähle von Baumaschinen und -fahrzeugen. Der Schaden für die betroffenen Unternehmen kann existenzgefährdend sein. Das LKA hat in diesem Bereich, nachdem Vertreter aus der Wirtschaft darum ersucht hatten, eine Sonderauswertung zu Diebstählen von Baumaschinen und -fahrzeugen im Land Sachsen-Anhalt für den Zeitraum 2001 bis Mitte 2007 durchgeführt. Dass diese Thematik eine nicht zu unterschätzende Brisanz aufweist, lässt sich schon dadurch belegen, dass die Anzahl der entwendeten Baumaschinen in Sachsen-Anhalt in 2006 im Vergleich zu 2005 um 40,6% angestiegen ist (von 187 auf 263). Die Anzahl der entwendeten Baufahrzeuge ging im Vergleich der Jahre 2005 zu 2006 zwar um die Hälfte zurück (von 51 auf 27), der Schadensmittelwert liegt hier jedoch bei etwa 28.300 Euro pro entwendetem Fahrzeug, wohingegen er bei den Baumaschinen wesentlich geringer ist (hier ist eine Spanne von 1.000 Euro bis 40.000 Euro je Delikt festzustellen).

Die am häufigsten entwendeten Baufahrzeuge sind übrigens Radlader, gefolgt von Baggern. Die Diebstähle von Baufahrzeugen und maschinen erfolgen fast ausschließlich auf offenen und frei zugänglichen Baustellen, Angriffe auf dem Unternehmensgelände sind hingegen weitaus seltener. Baufahrzeuge werden häufig durch das Kurzschließen der Zündeinheit oder unter Benutzung von universell



benutzbaren Seitenschlüsseln gestartet und vom Gelände bewegt. Oftmals werden sowohl Baufahrzeuge als auch Baumaschinen zugleich entwendet. Dabei ist vielfach der mit Baumaschinen beladene firmeneigene Lkw das Transportmittel bei der Tatbegehung.

Es konnte ermittelt werden, dass die Täter die gestohlenen Baufahrzeuge teilweise im Vorfeld auf den Baustellen photographiert, im Internet zum Verkauf eingestellt und bei Kaufwünschen von Interessenten unmittelbar nach dem Verkauf gestohlen und ausgeliefert hatten.



Bei den Baumaschinen ist das beliebteste Objekt die Rüttelplatte, dicht gefolgt von Notstromaggregaten. Es wird davon ausgegangen,

dass die Orte wo diese Geräte entwendet werden, gezielt von den Dieben aufgeklärt worden sind. Andere bei Baumaschinendiebstählen häufig entwendete Gegenstände sind Trennschneider, Bohrmaschinen und Sägen etc., diese werden meist aus Containern oder abgestellten Fahrzeugen gestohlen.

Bei einer weiteren Tatvariante setzen sich die Täter nicht durch Diebstahl sondern durch Betrug in den Besitz von hochwertigen Baumaschinen und Fahrzeugen, indem sie sie anmieten und nach der Anmietung häufig ins Ausland verkaufen. Mit dieser Vorgehensweise hat eine aus Brandenburg stammende Tätergruppe im Bereich der PD Stendal einen Radlader im Wert von 99.000 € erlangt und diesen anschließend über das Internet in die USA verkauft. Dies geschah, bevor der Vermieter in Deutschland Anzeige wegen des vermeintlichen „Diebstahls“ erstattete.

Zur Fahndung nach den entwendeten Fahrzeugen sind auch die lagebildabhängigen Kontrollen intensiviert worden. Besonders positiv wurde von der Bauwirtschaft der polizeiliche Vorschlag - Initiator war die PD Merseburg - aufgenommen, der Polizei die Einrichtung und den Standort von Großbaustellen im Vorfeld mitzuteilen. Denn bis dahin wurden den Beamten Baustellen oft erst bekannt, wenn Diebstähle zu verzeichnen waren.

Nur am Rande ist anzumerken, dass auch die Diebstähle von Buntmetallen, aber auch z. B. Kupferkabel seit einigen Jahren ganz erheblich zugenommen haben, die Schadenssumme die durch Metalldiebstähle in Sachsen-Anhalt im Jahr 2005 verursacht worden war, beläuft sich auf mehr als 1,8 Millionen Euro.

Kommen wir nun zu dem Kriminalitätsfeld das ich Ihnen bereits angekündigt hatte, nämlich dem großen Bereich bei dem der Computer und das Internet bei der Tatbegehung eine Rolle spielt. Die polizeiliche Bezeichnung für solche Delikte ist IuK-Kriminalität (Informations- und Kommunikations-Kriminalität).

III. IuK Kriminalität

Dass das Internet heutzutage auch aus dem Geschäftsleben nicht mehr wegzudenken ist, lässt sich an einigen, wie ich finde, eindrucksvollen Zahlen belegen: Nach Schätzungen von Marktforschungsunternehmen wird der elektronische Handel bis zum Jahr 2009 in Deutschland auf rund 694 Milliarden € ansteigen - im Jahr 2005 waren es noch 321 Milliarden €. 78% der Teilnehmer einer Umfrage unter deutschen Unternehmen, darunter viele mittelständische Betriebe, begreifen eBusiness und die damit verbundene Optimierung von Geschäftsprozessen bereits als Teil ihres Tagesgeschäfts. Zum Ende des Jahres 2006 erledig-

ten bereits 31,4 Millionen Deutsche Einkäufe über das Internet (Quelle: BSI, Die Lage der IT-Sicherheit in Deutschland). Der Anstieg dieser geschäftlichen Internetaktivitäten führt allerdings auch zu neuen Herausforderungen für die IT-Sicherheit.

Die Bedrohungen, denen die Nutzer von IT-Systemen ausgesetzt sind, sind überaus zahlreich und vergrößern sich fast täglich. Ich möchte aus diesem Grunde hier nur einige exemplarische Beispiele anführen:

Einen erheblichen Teil der Internetkriminalität machen Warenbetrugsdelikte mittels Internet aus (dies ist eine Schnittstelle von IuK- und Wirtschaftskriminalität, Warenbetrugsdelikte haben im Jahr 2006 auch den rasanten Anstieg der Wirtschaftskriminalität in Sachsen-Anhalt bewirkt). In diesem Deliktsbereich stellen sie den Hauptanteil der erfassten Straftaten dar. In Sachsen-Anhalt hat sich die Anzahl dieser Taten im Jahr **2006 (5278 Fälle)** gegenüber dem Jahr **2005 (2428 Fälle)** um fast **150%** erhöht. Beim Warenbetrug werden die angebotenen Waren zwar ausgeliefert aber nicht bezahlt oder die bereits bezahlte Ware wird nicht oder in schlechter Qualität geliefert, wobei die Verwendung fremder Identitäten (Accountmissbrauch) zugenommen hat. Im letzten Jahr gab es sowohl im Bereich der Polizeidirektionen Halle und Merseburg ein größeres Verfahren dieser Art, bei denen die bandenmäßig organisierten Täter mehrere hundert Personen geschädigt haben. Besonders zu nennen ist dabei der sog. Warenbetrug durch **Accountmissbrauch**.

Dazu folgender **Beispielfall** aus dem Jahre 2005: In Dessau erstattete ein Bürger beim dortigen Polizeirevier Anzeige, nachdem er ein Schreiben von einer Motorradfirma erhalten hatte, in dem ihm mitgeteilt wurde, er habe über das Internet ein Motorrad erworben. Der Mann hatte jedoch zu keinem Zeitpunkt eine solche Bestellung getätigt und besaß auch keinen Internetanschluss. Mit Hilfe eines Nachbarn, der über einen Internetanschluss verfügte, stellte er bei einer eBay-Recherche fest, dass eine unbekannte Person mit seinen Daten dort Einkäufe tätigte. Der Schaden bzw. die ausstehenden Beträge betrugen zu diesem Zeitpunkt bereits über 271.000 €. Der unbekannte Täter hatte unter dem Namen des Opfers u. a. einen Ferrari und das besagte Motorrad käuflich erworben. Der Geschädigte selbst verfügte seit 1994 über keinen Internetanschluss mehr, hatte aber ein Mitgliedskonto bei eBay eingerichtet und sein Passwort war noch unverändert. Wie der oder die unbekanntenen Täter an die Zugangsdaten gekommen waren, war konkret nicht festzustellen.

Zum Account-Missbrauch ist aus kriminalistischer Sicht folgendes zu sagen: Er dient entweder der betrügerischen Erlangung oder der betrügerischen Veräußerung von Waren. Beim Account Takeover erlangen die Täter entweder durch gefälschte E-Mails (Phishing)

oder durch systematisches und automatisches Ausprobieren von Passwörtern (Brute-Force-Zugriff) Zugriff auf die Accounts der Betroffenen/Geschädigten. In der Folge wird das Passwort des Betroffenen geändert und unter dem Account agiert (bei betrügerischen Verkäufen werden z. B. Bankdaten, Kontaktdaten geändert). Um möglichst kein Misstrauen aufkommen zu lassen, sind für die Täter Accounts von eBay-Mitgliedern besonders interessant, die bisher zu 100% positiv bewertet worden sind. Bemerkt der tatsächliche Account-Inhaber den Missbrauch, ist es ihm zunächst aufgrund des geänderten Passwortes nicht möglich, auf seinen Account zuzugreifen. Dem Betroffenen/Geschädigten verbleibt lediglich die Möglichkeit, eBay über das entsprechende Kontaktformular zu informieren, wobei die Reaktionszeit zwischen 24 und 48 Stunden betragen kann.

Damit der Online-Handel in Deutschland weiter wachsen kann, müssen sowohl die Unternehmen, als auch die Kunden Vertrauen in die Sicherheit des Internets haben. Informationen um den elektronischen Geschäftsverkehr sicherer zu gestalten, bietet das Ministerium des Bundes für Wirtschaft und Technologie auf seiner Internetseite an (BMWi-E-Business-Sicherheitsmaßnahmen). Für den Auf- und Ausbau internetbezogener Geschäftsfelder - gerade für mittelständische Unternehmer - werden fundierte Hinweise für mehr Sicherheit im Internet zur Verfügung gestellt.

Schadprogramme insbesondere Trojaner und Spyware

Computerschadprogramme stellen die häufigste Angriffsform gegen IT-Systeme dar. Die starke Verbreitung von Standardsoftware und die darin enthaltenen Sicherheitslücken in Standardapplicationen wie Office-Anwendungen oder Webbrowsern stellen eine ideale Angriffsfläche für die Verfasser von Schadprogrammen dar. Die Programme werden meistens über E-Mail Anhänge verbreitet. Die wichtigste Form sogenannter **trojanische Pferde** Programme, die ohne Wissen der Rechner aktiv werden und heimlich Schadfunktionen ausführen. Trojaner sind vielseitig einsetzbar, sie können fremde Rechner vollständig kontrollieren, Daten ausspionieren, Tastatureingaben und Bildschirmausgaben aufzeichnen. Nutzer die ihre Personalcomputer nicht mit den erforderlichen Sicherheitssystemen ausgestattet haben (fehlende Antivirensoftware, keine Firewall, Sicherheitslücken im Betriebssystem) sind für Schadprogramme besonders empfänglich. Die Gefahren, die durch den Einsatz von Spyware gerade auch für vertrauliche Unternehmensdaten bestehen, dürften auf der Hand liegen.



Weiterhin sind die elektronischen Spione als eine Unterform der Schadprogramme zu erwähnen; die sogenannte Spyware. **Spyware** nistet sich heimlich via Internet in Rechnern und Netzwerken ein, erkundet dort interessante Informationen und liefert diese über das Internet unbemerkt an andere weiter. Auf diese Weise lassen sich z. B. von Kunden des Online-Handels ganze Verhaltensprofile erstellen: Welche Internet-Seiten werden von den PC Nutzern vorzugsweise angeklickt? Welche Produkte oder Waren werden bestellt? Die digitalen Spione können sogar die Start Seite des Internet-Browsers ändern, so dass plötzlich Werbeseiten am Bildschirm auftauchen. Ein weiteres beliebtes Ziel sind die Favoritenordner des Browsers, die die Spyware unbemerkt um Zusatzseiten ergänzt.

Ein **Beispiel** für die Wirkungsweise von Schaden stiftenden Programmen ist in Sachsen-Anhalt im Jahr 2006 bekannt geworden: Der Geschädigte unterhält in Magdeburg einen Internetshop als selbständiger Gewerbetreibender. Zur Tatzeit befand er sich in einem Chatroom im Internet. Plötzlich öffnete sich auf dem Bildschirm seines PC ein Dialogfenster und meldete ihm, dass ein Servicepack auf seinem PC installiert werde. Dieses Servicepack war aber bereits früher vom Geschädigten installiert worden. Seine Versuche die Installation abubrechen oder den Rechner abzumelden, schlugen fehl. Dem Geschädigten wurde der Zugriff verweigert und ihm wurde mitgeteilt, die Nutzerrechte für das Servicepack seien bereits abgelaufen. Der Rechner hat sich schließlich selbst abgeschaltet. Der Geschädigte geht davon aus, dass sich jemand unberechtigt Zugriff auf seinen Rechner verschafft und dessen Daten auf der Festplatte gelöscht hat.

Eine besonders perfide Form der Datenveränderung bzw. der Computersabotage ist das Phänomen des **Datenkidnapping**. Hierzu verschaffen sich Hacker mit ganz bestimmten Trojanern Zugang zu fremden Computern, verschlüsseln auf diese Weise persönliche Daten auf der Festplatte und erpressen ein Lösegeld für deren Freigabe. Ziel ist es, die Datenbesitzer durch Drohung mit einer kompletten Löschung der Dateien einzuschüchtern und sie zur Zahlung der geforderten Summe zu veranlassen.

Erpressungsfälle dieser Art sind in Sachsen-Anhalt bisher noch nicht bekannt geworden, sie sind aber für die Zukunft durchaus denkbar. Es ist zu befürchten, dass, wenn solche Fälle eintreten, das Anzeigeverhalten betroffener Bürger bzw. Unternehmen gering wäre. Eine polizeiliche Ermittlung würde sich höchstwahrscheinlich auch auf die als „Geiseln“ einbehaltenen sensiblen Daten beziehen, die von den Betroffenen dann offenbart werden müssten. Das könnte eine große Anzahl von Opfern davon abhalten, Strafanzeige bei der Polizei zu stellen.

Ein Kriminalitätsphänomen welches zukünftig wahrscheinlich vor allem Unternehmen und Behörden vermehrt betreffen wird, sind sogenannte **Denial-of-Service-Attacken (DoS)**. Ein DoS-Angriff bezeichnet allgemein einen Angriff gegen die Verfügbarkeit eines IT-Systems oder Dienstes mit dem Ziel, zu verhindern, dass der Nutzer zum Beispiel Zugriff auf die Webseite eines Online-Shops nimmt. Technisch passiert dabei folgendes: Bei DoS Angriffen wird ein Server gezielt mit so vielen Anfragen „bombardiert“, dass das System die Aufgaben nicht mehr bewältigen kann und im schlimmsten Fall zusammenbricht.



Auf diese Art wurden schon bekannte Web-Server wie zum Beispiel Amazon, Yahoo, eBay, mit bis zur vierfachen Menge des normalen Datenverkehrs massiv attackiert und waren damit für ihre Kunden für geraume Zeit nicht mehr erreichbar.

Um die Datenmengen zu erhöhen und die Angriffe damit noch effektiver zu machen, haben die Hacker weltweit in den letzten Jahren zunehmend verteilte **(Distributed) Denial-of-Service-Attacken (DDoS)** durchgeführt. Dazu installieren die Hacker ihre Angriffsprogramme auf mehrere Rechner. Diese Rechner werden Kommando des Hackers greifen Wissen der Computerbesitzer, und mit gefälschten Anfragen, zum dadurch technisch überlastet wird

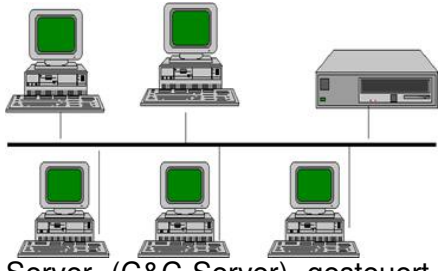


hundert bis tausend ungeschützte zum Angriffswerkzeug, denn auf sie gemeinsam an, allerdings ohne überschütten ein bestimmtes Ziel Beispiel einen Webserver, der und seinen Betrieb einstellt.

Sich vor solchen Angriffen zu schützen, ist deshalb schwer, weil der Zielrechner die Daten erst erhalten muss, um sie zu analysieren. Die Hacker selbst lassen sich nur schwer ermitteln, da sie in den meisten Fällen mit gefälschten IP-Quelladressen arbeiten. Bei laufenden Attacken besteht die Möglichkeit, Filterregeln an zentralen Netzkomponenten einzurichten, um zum Angriff gehörende Daten zu extrahieren und zu verwerfen. Ist das Ausmaß der Attacke so groß, dass bereits der Netzknoten überlastet ist, muss versucht werden in Kooperation mit dem Netz Provider zu treten. Häufig läuft dies auf ein Wettrennen zwischen Angreifer und Opfer hinaus.

Um DDoS Angriffe vornehmen zu können, bedienen sich die Täter sogenannter **Bot-Netze**. Von Bot-Netzen (Kurzform von Robot) spricht man, wenn ein Angreifer per Fernsteuerung sehr viele von ihm mit einer Schadsoftware infizierte PC - meist mehrere Tausend -

zusammenschließt und durch diese Schadsoftware (Malware) verbreiten lässt oder verteilte Attacken auf vom Angreifer vorgegebene Zielsysteme vornehmen lässt (DDoS Angriffe, s. o.). Bot Programme werden dem PC Anwender häufig über E-Mail Anhänge oder präparierte



Webseiten eingeschleust. Da ein mit einem Bot infizierter Computer den Befehlen des Angreifers gehorcht, werden diese angegriffenen PC häufig auch als „Zombies“ bezeichnet. Jeder einzelne Zombie Computer wird von einem Hauptcomputer dem Command-and-Control-Server (C&C-Server) gesteuert. Die mit einem Bot infizierten Rechner-Systeme bauen eigenständig eine Verbindung zu diesem Server auf und nehmen ihre Anweisungen von dort entgegen.

Die Betreiber von Botnetzen agieren weltweit und sind dabei so geschickt, dass die Einrichtung eines Botnetzes von den Opfern selten bemerkt wird. Die Einrichtung über Viren und Trojaner erfolgt dergestalt, dass der betroffene Zombie Rechner selbst nicht geschädigt wird. Die Schaden stiftende Software dient allein der Fernsteuerung des Rechners.

Trotz der überaus schwierigen Ermittlungssituation zeigen Gegenmaßnahmen Wirkung. Verstärkte Maßnahmen zur Aufklärung und Sensibilisierung der Privatanwender haben dazu geführt, dass Virens Scanner und Personal Firewalls sowie lokale Sicherheitsrichtlinien immer konsequenter eingesetzt und Updates regelmäßig installiert werden. Immer mehr Bürger erkennen wohl auch, dass sie ihr PC als Teil eines Bot-Netzes zu unfreiwilligen Tätern bei schwerwiegenden Delikten wie Wirtschaftsspionage oder Erpressung machen kann.

Sicherheitslösungen zum Schutz lokaler Netze gegen Angriffe jedweder Art werden neben einer Unzahl privater Anbieter auch durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Verfügung gestellt. Das BSI gibt dabei Informationen zu Firewalls, Anti-Viren-Programmen usw., sowie zu Verfahren, die der Absicherung des Datentransports dienen.

III. Produkt- und Markenpiraterie

Kommen wir nun zu einem anderen Deliktsbereich, der im letzten Jahr eine Steigerung der Fallzahlen zu verzeichnen hatte. Zugenommen hat in Sachsen-Anhalt wie auch bundesweit die Zahl der Straftaten gegen den freien Wettbewerb, zu nennen ist hier insbesondere die **Produkt- und Markenpiraterie**. Bei den letztgenannten Straftaten die das Rechtsgut des geistigen Eigentums beeinträchtigen, ist die kriminelle Energie der Täter überaus hoch, sie besitzen bei ihren Handlungen praktisch kein Unrechtsbewusstsein.

Generell ist festzustellen, dass es heutzutage keine Produkte mehr gibt, die nicht gefälscht werden. Die Palette reicht von Kosmetika, über Textilien und Tonträgern bis hin zu Medikamenten. Die Produzenten dieser Falsifikate stammen dabei überwiegend aus Südostasien, insbesondere aus China. Bei dem Vertrieb der Falsifikate spielt das Internet wiederum eine große Rolle. Die Zeiten, als die Täter z. B. versuchten, gefälschte Sportbekleidung namhafter Hersteller auf dem Flohmarkt zu verkaufen sind wahrscheinlich endgültig vorbei. Heutzutage wird ein großer Teil der gefälschten Ware auf virtuellen Marktplätzen feilgeboten.

Vor einigen Jahren hatte die Polizeidirektion Magdeburg einen Fall dieser Art zu bearbeiten (Ermittlungsgruppe Joop). In 2004 erstattete eine Rechtsanwaltskanzlei bei der PD Magdeburg Strafanzeige wegen Betruges. Eine Mandantin dieser Kanzlei hatte zuvor im Internetauktionenhaus eBay ein als Originalware ausgewiesenes JOOP Schmuckstück ersteigert, welches jedoch, wie sich nachträglich herausstellte, gefälscht war. Die späteren Ermittlungen, Ansatzpunkt war der Accountname des Verkäufers, ergaben Hinweise auf 69 Personen im In- und Ausland. In einer konzertierten Aktion von Polizei, Steuerfahndung und Zoll wurden umfangreiche Durchsuchungsmaßnahmen in Deutschland, Österreich und der Türkei durchgeführt. Nach den Ermittlungen hatten die Täter über 76.000 Artikel unter den Originalnamen „JOOP“, „Prada“, „Gucci“ über das Internet versteigert. Die Fälschungen waren in der Türkei hergestellt worden, die Haupttäter waren türkische Staatsangehörige. Bei der Analyse der Konten der Täter wurden Geldflüsse von ca. 1,3 Millionen Euro festgestellt. Diese Bande konnte zerschlagen werden, aber es ist natürlich davon auszugehen, dass dies nur die „Spitze des Eisberges“ ist.

Die derzeitige Entwicklung der Wirtschaft wird auch weiterhin für Steigerungen in diesem Deliktsfeld sorgen. Strafanzeigen oder Hinweise auf Verstöße gegen das Urheberrechtsgesetz etc. gehen - neben den polizeilichen Erkenntnissen - hauptsächlich durch die Inhaber der Schutzrechte bzw. deren Rechtsanwälte, den Aktionskreis Deutsche



Wirtschaft gegen Produkt- und Markenpiraterie e. V. (APM) sowie durch die Piratenverfolgungsgesellschaften BSA, GVU, IFPI und GEMA ein. Mit ihnen besteht eine enge Zusammenarbeit. Ein effektives Mittel zur Bekämpfung der Produktpiraterie stellt die Einziehung der Produkte und Tatmittel dar. Die gefälschte Ware wird nach dem Urteil oder nach außergerichtlicher Einziehung

vernichtet, technische Geräte werden versteigert.

Insgesamt liegen die Möglichkeiten der präventiven Bekämpfung der Produktpiraterie weniger bei der Polizei als bei der Wirtschaft. So sind z. B. die betroffenen Unternehmen der Softwareindustrie aufgefordert, nicht nur effiziente Verschlüsselungs- und Kopierschutzsysteme sowie offene und verdeckte fälschungssichere Kennzeichnungen für ihre Markenartikel zu entwickeln, sondern auch bereits bekannte Präventionsmöglichkeiten zu nutzen.

IV. Korruptionsstraftaten

Gestatten Sie mir noch ein Wort zu den **Korruptionsstraftaten**. Die reinen Fallzahlen in Sachsen-Anhalt sind gering (in den letzten Jahren, mit Ausnahme 2006 fast regelmäßig im zweistelligen Bereich). Sie alle haben sicherlich die jüngste Berichterstattung in den Medien über Korruptionsverdacht bei namhaften deutschen Unternehmen mitverfolgt. Die polizeilichen Statistiken sprechen insoweit allerdings eine andere Sprache. Laut Bundeslagebild Korruption **2006** ist das Hauptzielfeld der Korruption die öffentliche Verwaltung **64,4%** und nur zu **29%** die Privatwirtschaft. Bei den Strafverfolgungsbehörden ist der Fokus immer noch überwiegend auf die Bestechung / Bestechlichkeit bei Amtsträgern gerichtet (insbesondere Begünstigung bei Ausschreibungen).

Das LKA Sachsen-Anhalt hat zum Beispiel im Jahr **2005** nach über fünfjähriger Bearbeitungszeit die Ermittlungen gegen einen Projektmanager der deutschen Bahn AG abgeschlossen. Dieser war seit Anfang der 90er Jahre für die Prüfung von Ausschreibungsunterlagen und Vorbereitung der Vergabe von Bauleistungen (Investitionsvolumen 510 Millionen Euro) im Bereich der neuen Länder zuständig. Er und seine Mittäter hatten ein korruptives Netzwerk zu namhaften Bauunternehmen aufgebaut. Um eine unauffällige Bezahlung der korruptiven Leistungen (Einnahmen etwa 3,5 Millionen DM) zu gewährleisten hatten sie mehrere Scheinfirmen gegründet. Diese Scheinfirmen stellten gegenüber den Bauunternehmen Rechnungen über fiktive Beratungsleistungen aus. Die Beteiligten wurden zu hohen Freiheitsstrafen bzw. Geldstrafen verurteilt.



Nach Ansicht des BKA, und ich teile diese Ansicht, ist das schon traditionell bestehende Übergewicht der Korruptionsfälle in der allgemeinen öffentlichen Verwaltung nicht zwingend ein Beleg für die besondere Korruptionsanfälligkeit dieses Sektors im Vergleich zur Privatwirtschaft. Vielmehr ist davon auszugehen, dass trotz einer zunehmend feststellbaren Sensibilität und Aufklärungsbereitschaft der Unternehmen die Zahl der Korruptionsfälle in der Privatwirtschaft weitaus höher ist, als die Fallzahl in der polizeilichen Statistik erwarten lässt. Ursächlich für die Haltung der Unternehmen dürfte sein, dass sie bei aufgedeckten

Korruptionsfällen aufgrund des erwarteten Imageschadens primär unternehmensintern gegen die Verantwortlichen vorgehen.

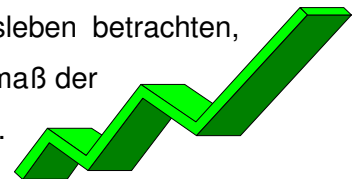
V. Informationsaustausch zwischen Polizei und Wirtschaft

Ich habe Ihnen jetzt einige Aspekte der Kriminalitätsentwicklung vorgestellt. Die Daten beruhen auf den Feststellungen wie sie aus unseren polizeilichen Lagebildern zu entnehmen sind. Neben diesen statistischen Daten ist es aber auch immer nützlich, das Sicherheitsgefühl der von Kriminalität Betroffenen zu untersuchen. Es gilt also zu fragen, wie die Unternehmer selbst die Bedrohung durch Kriminalität einschätzen. Aufschlussreich ist insoweit eine im Jahr **2006** von der Wirtschaftsprüfungsgesellschaft **KPMG** verfasste Studie zur Wirtschaftskriminalität in Deutschland. Wobei anzumerken ist, dass die Verfasser dieser Studie dann von Wirtschaftskriminalität ausgehen, wenn zu Lasten eines Unternehmens Straftaten verübt worden sind. Nach polizeilicher Begriffsbestimmung liegt Wirtschaftskriminalität hingegen nur dann vor, wenn der Täter im Rahmen eigener wirtschaftlicher Betätigung handelt und eine Vielzahl von Personen oder die Allgemeinheit schädigt.



Von den repräsentativ befragten Unternehmensverantwortlichen gaben insgesamt **71%** an, dass sie das Phänomen Wirtschaftskriminalität als ein ernsthaftes Problem für das Wirtschaftsleben betrachten, **62%** glaubten darüber hinaus, dass das Ausmaß der

Wirtschaftskriminalität in der nächsten Zeit noch zunehmen wird.



Die häufigsten Delikte die in den Unternehmen begangen wurden sind Diebstahl / Unterschlagung, Untreue und Betrug. Betroffen waren vorrangig die geldnahen Prozesse der befragten Unternehmen (Einkauf, Vertrieb, Lager, Produktion sowie Finanzen).

Auch wenn es sich bei der vorliegenden Studie von KPMG um eine Bundesstudie handelt, dürften die Ergebnisse auf die Verhältnisse in Sachsen-Anhalt übertragbar sein.

Die überwiegende Anzahl der Unternehmer besitzt folglich im Hinblick auf Wirtschaftskriminalität ein hohes **Problembewusstsein**. Auf der anderen Seite ist es ein offenes Geheimnis, dass sich viele Verantwortliche aus der Wirtschaft davor scheuen, die Ermittlungsbehörden zu kontaktieren, wenn sie entdeckt haben, dass ihr Unternehmen das Opfer von Kriminellen geworden ist. Nicht wenige Geschädigte ziehen es vor, keine Strafanzeige zu erstatten, sondern klären die Angelegenheit lieber intern. Wenn es sich bei den Tätern um Angehörige des eigenen Unternehmens handelt, werden vielfach ausschließlich arbeits- oder zivilrechtliche Mittel angewendet. Ursächlich für dieses Verhalten ist die Angst vor geschäfts-

schädigendem Imageverlust und/oder mangelndes Vertrauen in die Aufklärungsarbeit der Strafverfolgungsbehörden.

Besonders fatal ist diese Vorgehensweise dann, wenn es sich bei Tätern aus dem eigenen Unternehmen um Personen aus dem sogenannten Topmanagement handelt. Nach einer wissenschaftlichen Studie, die unter Mitwirkung der Martin-Luther-Universität in Halle-Wittenberg erstellt worden ist, wird bei deliktischem Verhalten von Angehörigen dieser Personengruppe nur in Ausnahmefällen eine Strafanzeige erstattet. Eine derartige Privilegierung von Führungskräften ist verhängnisvoll, sie dürfte bei den übrigen Mitarbeitern die weit verbreitete Überzeugung verstärken, „dass man die Kleinen hängt, aber die Großen laufen lässt“.

Aus den angeführten Gründen sollte man sich als Unternehmer gut überlegen, wie mit strafbaren Vorfällen umzugehen ist. Es ist zwar richtig, dass keine Pflicht des Geschädigten besteht, Strafanzeige zu erstatten, ebenso richtig ist es aber auch, dass die strafrechtliche Aufklärung eines Sachverhaltes unbestreitbare Vorteile besitzt. Nur über das staatliche Zwangsinstrumentarium können sonst unbekannt bleibende Täter, Beweismittel sowie geheime Vermögenswerte aufgespürt und die Durchsetzbarkeit der Schadensersatzansprüche des Geschädigten verbessert bzw. gesichert werden.

Auch sollte jeder verantwortungsvolle Unternehmer ein Interesse daran haben, dass aus Gründen der Abschreckung und der Prävention zukünftigen kriminellen Verhaltens, die Täter einer adäquaten strafrechtlichen Sanktion zugeführt werden.

Entdeckungswege, Kontroll- und Präventionsmaßnahmen in den Unternehmen

Damit Unternehmen, die Opfer von Straftaten geworden sind, diese Delikte der Polizei anzeigen, müssen sie diese Straftaten jedoch erst einmal entdeckt haben. Auf welche Weise eine Straftat entdeckt wird, hängt sehr davon ab, ob es sich um einen internen oder einen externen Täter handelt. Bei Kunden, Geschäftspartnern oder Tätern ohne jegliche Geschäftsbeziehung zum Unternehmen werden die Delikte von Verantwortlichen eher durch externe Hinweise entdeckt, bei Tätern aus dem eigenen Unternehmen sind dagegen interne Hinweise und die interne Revision die häufigsten Entdeckungswege. PricewaterhouseCoopers hat im Jahr 2005 eine Studie zur Wirtschaftskriminalität herausgegeben, welche belegt, dass in Deutschland 66% der betroffenen Unternehmer nur deswegen von Straftaten Kenntnis erlangen, weil sie Hinweise von externen und internen Tippgebern erhalten oder Zufälle eine Rolle spielen. Diese Zahl belegt meines Erachtens, wie wichtig ein effektives

Kontrollsystem ist. Die meisten Unternehmen verfügen zwar über eine interne oder externe Revision, dies scheint aber nicht ausreichend zu sein.

Ein Weg der von den Unternehmen daher zunehmend häufiger beschritten wird, ist es Hinweisgebersysteme (z. B. sog. Hotlines, wobei sich als Medium nicht nur Telefon, sondern auch e-Mail empfiehlt) einzuführen. Sie erhöhen nachweislich die Chance, Verdachtsmomenten möglichst früh nachgehen zu können. Im internationalen Vergleich zeigte sich, dass Unternehmen, die über eigene funktionierende Hinweisgebersysteme verfügen, deutlich weniger von externen Hinweisgebern oder externen Ermittlern abhängig waren. Insbesondere Korruption und Bestechung konnten hierdurch häufiger aufgedeckt werden. 23% der deutschen Unternehmen bieten mittlerweile derartige Kommunikationswege an. Die häufig befürchteten innerbetrieblichen Widerstände und Konflikte sind nahezu ausgeblieben. Weniger als 5% der Unternehmen berichten über Probleme bei der Einführung eines Hinweisgebersystems. Dies setzt aber voraus, dass mit derartigen Systemen verantwortungsvoll umgegangen wird und klare und nachvollziehbare Prozesse definiert sind. Es muss klar ausgeschlossen werden können, dass das System zur Denunziation missliebiger Kollegen missbraucht werden kann.

Möglichkeiten die der Wirtschaft zur Verfügung stehen, um Kriminalität von den Unternehmen abzuwenden möchte ich hier nur Stichwortartig erwähnen: unbedingt notwendig ist es meiner Ansicht nach, Risiko- und Gefährdungsanalysen zu erstellen und die vorhandenen aufbau- und ablauforganisatorischen Maßnahmen auf ihre Effektivität hin zu überprüfen: ich nenne nur Vier-Augen-Prinzip, Berechtigungskonzepte und Datensicherungen oder Konzepte der Zugangs- und Zutrittssicherheit.

Zu guter Letzt möchte ich noch eine weitere Maßnahme ansprechen, auch wenn diese vielfach belächelt wird: Sensibilisierung der Mitarbeiter durch Schulung von Sicherheitsbestimmungen. Die vom mir bereits angesprochene Studie von KPMG stellt fest, dass gut die Hälfte der von Wirtschaftskriminalität betroffenen Unternehmen davon ausgeht, dass mit einer erhöhten Sensibilisierung der Mitarbeiter und des mittleren Managements bzgl. Wirtschaftskriminalität die Verhütung dieser Straftaten möglich gewesen wäre. In einer Erweiterung einer alten Spruchweisheit dürfte damit feststehen, dass gut ausgebildete und motivierte Mitarbeiter nicht nur der größte Schatz eines Unternehmens sind, sondern dem Unternehmen selbst auch den größten Schutz vor Kriminalität gewährleisten.

VI. Der Beitrag der polizeilichen Beratungsstellen für die Unternehmenssicherheit

Der Bereich der Verhinderung von Straftaten stellt einen wichtigen Beitrag der polizeilichen



Arbeit dar. Die rechtliche Grundlage für die Prävention ist das Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt (SOG LSA). Alle Polizeidirektionen und das LKA verfügen über spezielle Fachbereiche die sich dieser bedeutsamen Materie widmen. Das Tätigkeitsfeld der polizeilichen Kriminal-

prävention ist überaus umfangreich, genannt seien hier nur die Verhinderung von Kinder- und Jugendkriminalität, Drogenprävention und Schutz des Eigentums. Dem letztgenannten Bereich kommt naturgemäß eine große Bedeutung zu, er bildet traditionell einen der Hauptschwerpunkte der Präventionsarbeit. Wenn man über Schutz des Eigentums spricht, meint man damit speziell den Schutz des Wohneigentums vor Einbruchsdiebstahl. Es dürfte kaum einen Kriminalitätsbereich geben, der das Sicherheitsbedürfnis der Bürger so stark beeinträchtigt wie der Wohnungseinbruch. Wer schon einmal das Opfer eines Wohnungseinbruches geworden ist, weiß, dass das Schlimmste an diesem Vorfall nicht so sehr der Verlust von Wertgegenständen ist, sondern vielmehr der massive Einbruch in die Privatsphäre, der die Opfer teilweise noch jahrelang verfolgt.



Im Hinblick auf die Bedeutung des Delikts Einbruchsdiebstahl verfügen die Polizeidienststellen über umfangreiches Informationsmaterial und kompetente Ansprechpartner die zu allen Varianten moderner Sicherheitstechnik, sowie zu richtigem Verhalten wertvolle Hinweise geben können. Der Expertenrat kommt dabei natürlich nicht nur den einfachen

Bürgern zugute, sondern in gleicher Weise Einzelgewerbetreibenden und Unternehmen, denn erfahrungsgemäß suchen sich die Einbrecher nicht nur Einfamilienhäuser und Wohnungen als Ziele aus, sondern genauso gefährdet sind Lager und Produktionshallen, Ladengeschäfte, Handwerksbetriebe und Kanzleien etc. Für alle Ratsuchenden besteht die Möglichkeit, die gefährdeten Objekte durch die für technische Prävention zuständigen Mitarbeiter der Direktionen besichtigen zu lassen, damit diese eine Analyse der vorhandenen Sicherheitsrisiken und Schwachstellen vornehmen. Die Kollegen überprüfen dabei u. a. die mechanischen Sicherungen, informieren über personelle und organisatorische Maßnahmen und geben Tipps zu richtigem Verhalten. Da das Thema Einbruchschutz und Sicherheitstechnik heute noch ausführlich durch kompetente Referenten behandelt werden wird, möchte

ich Sie zur Vermeidung von Wiederholungen auf deren Redebeiträge verweisen. Gleichzeitig möchte ich die Gelegenheit nutzen und ihnen an dieser Stelle anhand von Beispielen die Präventionsaktivitäten einzelner Polizeidirektionen darstellen, deren Arbeit in der Öffentlichkeit häufig nicht in ausreichendem Maße gewürdigt wird.

Ausgesuchte Mitarbeiter des Dezernats 12 (Prävention) aller sechs noch bestehenden Direktionen haben in der Vergangenheit regelmäßig Sicherheitsberatungen und Schwachstellenanalysen bei Handwerksbetrieben, kleinen mittelständischen Unternehmen sowie in Einzelhandelsgeschäften durchgeführt. Die beratenen Unternehmen stammen dabei, wie z. B. in der Direktion Halle aus allen Branchen: vom Optiker, über den Tiefbaubetrieb bis hin zum Kompostwerk. Hervorheben möchte ich auch die Polizeidirektion Dessau: Die Direktion Dessau hat im Januar 2007 mit dem Vorsitzenden der Firmenvereinigung des Kreisverbandes Anhalt-Zerbst und Dessau im Unternehmerverband Deutschland e. V. dem 480 Betriebe angehören, eine Konzeption zur Schwachstellenanalyse und Verhaltensprävention in Betrieben erarbeitet. Mitarbeiter derselben Direktion schulen Mitarbeiter von großen Ladenketten in einem Verhaltenstraining zu den Themen „Griff in die Kasse“, „Bedrohung“ und dem richtigen Verhalten bei Ladendiebstahl. Zwei Mitarbeiter der Direktion Magdeburg führen monatlich etwa 30 bis 40 Beratungen durch bei denen sie kleinere Firmen auf Schwachstellen hinweisen und eine entsprechende Analyse erarbeiten. Die Präventionsmitarbeiter aller Direktionen stellen bei ihrer Arbeit leider immer wieder fest, dass die Beratungsnachfrage bei den Unternehmen häufig erst dann entsteht, wenn das „Kind in den Brunnen gefallen“ d. h. das entsprechende Unternehmen das Opfer von Kriminellen geworden ist. Auch in Unternehmerkreisen (Anwesende natürlich ausgenommen) wird der Faktor Sicherheit anscheinend nicht immer in seiner ganzen Brisanz erkannt.

Das Vorgenannte mag zur Illustration der Arbeit der Direktionen ausreichen. Gestatten Sie mir noch einen Blick auf die Präventionsarbeit des LKA. Wie Sie sich vorstellen können, muss es, wenn verschiedene Dienststellen mit der Wahrnehmung der gleichen Aufgabe betraut sind, unter ihnen eine Arbeitsteilung geben. Die technische Prävention des Landeskriminalamtes steht daher in erster Linie dem staatlichen Bereich, d. h. den Landesbehörden, Justizeinrichtungen, Museen, sakralen Einrichtungen etc. in allen Fragen der Sicherheit in beratender Weise zur Verfügung. Die zuständigen Mitarbeiter des Dezernats Prävention meiner Behörde geben z. B. Empfehlungen ab, wie die Fenster und Fassaden von öffentlichen Einrichtungen beschaffen sein müssen, mit welchen Arten von Überfall- und Einbruchmeldeanlagen die Dienststellen auszustatten sind und wie die Überwachung der staatlichen Liegenschaften vorgenommen werden sollte. Wirtschaftsunternehmen berät das

LKA grundsätzlich nur dann, wenn diese Einrichtungen von strategischer Bedeutung für die Infrastruktur sind z. B. Flughäfen, große Gasversorger etc.

Trotz der geschilderten Aufgabenverteilung leistet auch das LKA einen konkreten Beitrag zur Unternehmenssicherheit: die mobile Beratungsstelle des LKA (Präventionsmobil). Diese bietet u. a. sicherungstätigkeit zur Verbesserung wie elektroan. Das Präventionsmessen und Ausstellungen von Verbänden, vertretungen und kann



technische Beratungserung des mechanischen Grundschutzes mobil besucht Gewebestellungen, Veranstaltungen, Berufs- und Interessenüber die Reviere,

Beratungsstellen der Polizei und das LKA, Dezernat 12 angefordert werden.

Ich hoffe, dass ich Ihnen mit diesen kurzen Ausführungen einen Überblick über die Präventionsarbeit in der Polizei geben konnte. Wie sie vielleicht in der Presse mitverfolgt haben, unterliegt die Polizeistruktur in Sachsen-Anhalt gerade einer Umorganisation. Als deren wichtigstes Ergebnis wird die Anzahl der Direktionen von sechs auf drei reduziert werden. Diese Umorganisation wirkt sich auf alle Arbeitsbereiche der Polizei und damit natürlich auch auf die polizeilichen Präventionsstellen aus. Ich vertraue jedoch darauf, dass unsere bewährten Beamten in den Dienststellen im Lande auch mit dieser Herausforderung fertig werden und auch zukünftig in bewährter Art und Weise ihre verdienstvolle Arbeit weiter fortführen.

Danke für die Aufmerksamkeit.