An den Landtag Nordrhein-Westfalen,
Platz des Landtags 1,
40221 Düsseldorf

Tobias Morsches
Dipl.Ing Informationstechnik (BA)
Freiheit 8a
51429 Bergisch Gladbach
tobias.morsches@add-yet.de

Betreff: Whistleblowing und PRISM - Anhörung A09 - 06.02.2014

Sehr geehrte Damen und Herren,

im Folgenden werde ich Ihre Fragen auf Basis meiner langjährigen Erfahrung als Angestellter IT-Forensiker und Penetration-Tester beantworten. Ich versichere Ihnen die Fragen nach bestem Wissen und Gewissen zu beantworten. Bitte haben Sie Verständnis, dass ich aus Sicherheitsgründen weder Kundennamen noch konkrete Schwachstellen benennen kann.

Sollten über die mündliche Anhörung hinaus noch Fragen offen sein, beantworte ich diese gerne auch zu späteren Zeitpunkten.

Mit freundlichem Grüßen

Tobias Morsches

Betreff: Whistleblowing und PRISM - Anhörung A09 - 06.02.2014

Zusammenfassung

Bereits Edward Snowden lies im Interview(ausgestrahlt am 26.01.2014 – ARD) anklingen, dass auch eine Überwachung von Kommunen und kommunalen Politikern stattfindet.

Die allgemeine Sicherheits-Lage in der öffentlichen Verwaltung ist kritisch. In allen von uns untersuchten Kommunen war es möglich vor Ort ohne Ausweis Geräte zu installieren und so einen Zugang zum Netzwerk zu erlangen. Bei fast allen Kommunen gelang es innerhalb von 2-8 Stunden, ohne Insider-Kenntnisse einen vollständigen Zugriff auf alle relevanten Systeme der betroffenen Kommunen zu erlangen. Diese Zugänge blieben über Wochen (teilw. Monate) unbemerkt. In vielen Fällen fehlten essentielle Sicherheitsmaßnahmen. Das notwendige Know-How für solche Angriffe ist über das Internet verfügbar. Doch selbst wenn technische Schwachstellen geschlossen sind, sind eingesetzte Systeme so aufgebaut, dass ein implizites Vertrauen zu den Herstellern der Software, sowie zu diversen Regierungen und Firmen besteht. Daher sind diese Institutionen (z.B. mittels Updates) in der Lage die Systeme zu kompromittieren.

Ein lesender und **schreibender** Zugriff besteht dabei auf Daten und Systeme wie z.B.:
- komplette Personenregister
- detaillierte Informationen über ansässige Ausländer
- gesonderte Listen mit Alias-Identitäten (z.B. gefährdete Personen)
- Daten des Ordnungsamts
- Daten der Finanzverwaltung
- Ratsinformationssysteme
- Schüler Leistungsdaten
- Alarmierungs-- und Leitsysteme der Feuerwehr

In NRW gibt es einen Fall, bei dem ausländische Geheimdienste verdächtigt werden. Dabei wurde eine Kommune angegriffen und man hat versucht von dort aus auf Systeme der Länder oder des Bundes zuzugreifen.

Bevor überhaupt über den Schutz vor Geheimdiensten nachgedacht werden kann, muss zunächst eine Basissicherheit hergestellt werden. Bei der Absicherung der Systeme macht es grundsätzlich Sinn zunächst vorhandene Möglichkeiten zu nutzen .Ein effektives Sicherheits-Konzept und die qualifizierte Umsetzung von IT-Sicherheitsmaßnahmen, sind oft wichtiger als technische Programm-Merkmale. Die effektivste Sicherheitsmaßnahme ist Datensparsamkeit und Datenvermeidung (§3a BDSG) durchzusetzen.

Eine weitere unverzichtbare Maßnahme ist eine effektive Verschlüsselung der Daten bei der Übertragung. Zum Beispiel auch für sensible (Email-)Kommunikation mit dem Bürger. Dabei wird oft darauf verwiesen, dass diese Mails nicht auf Viren geprüft werden können. Was faktisch nicht ganz korrekt ist. Allerdings müssen z.B. die Archivierung und Vertreterregelungen berücksichtigt werden. Auch müssen unterschiedliche Anforderungen innerhalb einer Kommune betrachtet werden. Das sind allerdings keine Probleme.

Grundsätzlich ist eine dezentrale Struktur einer zentralen Struktur aus folgenden Gesichtspunkten vorzuziehen:
- ein Angreifer benötigt mehr Aufwand um an weniger Daten zu gelangen
- ein dezentraler Ausfall verursacht weniger Kosten als ein zentraler
- kleine dezentrale Einheiten lassen sich besser kontrollieren
- das Missbrauchspotential zentraler Lösungen durch Einzelne ist relativ hoch
  (Ich kenne Mitarbeiter der öffentlichen Verwaltung die Ihre Bußgeldbescheide selbst löschen)

Ein Datenschutzprogramm sollte sowohl technische als auch organisatorische Vorgaben und Maßnahmen enthalten und diese den Mitarbeitern vermitteln. Darüber hinaus sollte es regelmäßige Kontrollen der Einhaltung geben.

Kann es sich NRW leisten auf **effektive** IT-Sicherheitsstandards zu verzichten?

Der Staat ist verpflichtet die Grundrechte seiner Bürger zu schützen. Daher sind IT-Sicherheitsmaßnahmen und Datenschutz für den Schutz der Bürger und ihrer Grundrechte unerläßlich. Es können z.B. beim Zeugenschutz auch Leben davon abhängen, dass Daten nicht an die Öffentlichkeit gelangen. Hier sollte man auch beachten, dass bestimmte Informationen beim Urlaub in anderen Ländern, ggf. anders zu bewerten sind.

Darüber hinaus hält die öffentliche Verwaltung auch diverse Daten zu geplanten Bauvorhaben und Subventionen oder anderen aus wirtschaftlichem Gesichtspunkten interessanten Entwicklungen.

Betreff: Whistleblowing und PRISM - Anhörung A09 - 06.02.2014

Detaillierte Beantwortung der Fragen

1. *Wie schätzen Sie die Gefahr ein, dass nordrhein-westfälische Landesbehörden bzw. kommunale Stellen von ausländischen Geheimdiensten überwacht und ausspioniert werden?*

a) <u>Der Begriff Überwachung/Spionage</u>

Zunächst einmal möchte ich darauf hinweisen, dass die Begriffe „Überwachung“ und „Spionage“ aus meiner Sicht nur ein Teilgesichtspunkt ist. Wie das Bundesverfassungsgericht 2008 bei der Schaffung des „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ geht es nicht nur um Vertraulichkeit, sondern auch um die Integrität. Geheimdienste können z.B. auch Manipulationen an Systemen und Daten der öffentlichen Verwaltung durchführen um Personen zu diskreditieren.

b) <u>Die aktuelle Sicherheitslage in der öffentlichen Verwaltung</u>

Im Rahmen der von mir und unserer Firma durchgeführten Sicherheitsüberprüfungen auf zahlreiche Systeme der öffentlichen Verwaltung erhielten wir, in fast allen Fällen, binnen kürzester Zeit (ca. 2-8 Stunden), ohne vorherige Kenntnisse der IT, vollen Zugriff auf alle Systeme der jeweiligen Kommunen oder Behörden. Es wurden sowohl Angriffe über das Internet, als auch Angriffe auf lokale Infrastrukturen durchgeführt. Teilweise sind von dort aus auch Zugriffe in andere Kommunen, zu kommunalen Dienstleistern oder Landes- und Bundes-Verfahren möglich. Im Rahmen der Überprüfungen waren auch auf diesen Systemen gravierende Schwachstellen sichtbar. Diese Schwachstellen werden allerdings von uns auf Grund des „Auftragsumfang“ nicht angegriffen.

Selbst einfachste Sicherheitsmaßnahmen sind oft nicht umgesetzt. Auf Grund der hohen Kosten für die Anpassung von Spezial-Software der Verwaltung, wird diese nur selten gegen bekannte Schwachstellen geprüft, dagegen abgesichert oder auf aktuelle Systeme portiert. Viele Applikationen setzen unsichere Konfigurationen oder unsichere Standard-Software voraus. Selbst die Bundesdruckerei verlangt(e) den Einsatz unsicherer Software (häufigste Infektionsquelle). Dadurch können die Systeme einfach mit Schadsoftware infiziert werden.

Wenn Verfahren oder Dateiablagen überhaupt mit Paßwort gesichert sind, ist dieses Paßwort oft leicht zu raten. Viele Daten liegen im Netzwerk und sind teilweise nicht einmal mit Paßwort gesichert. Alternativ sind die Paßwörter, für die Datenbanken der Verfahren für jedermann lesbar.

Ein Zugriff war in vielen Fällen sowohl aus dem internen Netz als auch über Internet möglich.

Im Größenvergleich schneiden die kleinen Kommunen mit ca. 2-3 IT-Mitarbeitern auf 50-60 Angestellte oft deutlich besser ab als größere Kommunen. Trotzdem ist auch hier ein Zugriff auf alle Systeme binnen kurzer Zeit möglich. Auch werden viele Verfahren an Dienstleister ausgelagert. Diese kommunalen Dienstleister stehen oft stark unter Druck und verzichten auf essentielle Sicherheitsmaßnahmen um Kosten zu sparen und Projekte schneller abzuschließen. Oft werden Verfahren mehreren Kommunen, ohne wirksame Trennung, in einem System verwaltet.

Diese Hürden sind selbst von Hobby-Hackern leicht zu meistern. Alle benötigten Tools und Anleitungen sind für Personen, die ihre eigene Sicherheit prüfen möchten, im Netz verfügbar.

c) IT-Sicherheitslage nach schließen „aller bekannten Schwachstellen“

Auch wenn die Schwachstellen geschlossen sind, sind die Systeme nicht Geheimdienst-sicher. Ausländischen Geheimdienste und Behörden und Behörden können sich die Schlüssel (Echtheits-Siegel) besorgen und so manipulierte Updates nutzen um Schadsoftware unterzuschieben. Für die betroffenen Städte ist es bei der Anzahl der Aktualisierungen und der Komplexität dieser nicht möglich alle „Aktualisierungen“ zeitnah zu prüfen. Die Aktualisierungen nicht zu installieren, öffnet Schwachstellen, die von jedermann ausgenutzt werden können, sie ungesehen zu installieren erlaubt allen Besitzern von „vertrauenswürdigen“ Schlüsseln die Kontrolle über die Systeme. Wer vertrauenswürdig ist definiert in der Regel der Hersteller der Software oder der Hersteller des Betriebssystems.

Nicht nur bei Aktualisierungen kommen diese „implizierten Vertrauensstellungen“ zum Einsatz. In vielen Fällen werden Verbindungen über zentrale Vertrauensstellungen abgesichert. Dabei sind für viele Systeme Listen mit vertrauenswürdigen Ausstellern vordefiniert. Zu diesen Ausstellern gehören neben den kommerziellen Ausstellern auch staatliche Stellen, große Firmen, Universitäten und andere Institutionen. Jede dieser Institutionen kann dann entsprechende „Ersatz-Schlüssel“ ausstellen, welche es Angreifern unbemerkt erlauben den Datenverkehr zu lesen oder zu verändern.

Selbst wenn die Geheimdienste nicht über die Schlüssel verfügen, benötigt der Hersteller bei bekanntwerden einer Schwachstelle Zeit diese zu schließen. Im Rahmen von speziellen Programmen, besteht ein „Frühwarnsystem“ für besondere Kunden (z.B. Regierung und Geheimdienste). Diese erhalten alle Informationen zu einer Schwachstelle, sobald der Hersteller diese bekommt. Dadurch können sie ggf. Maßnahmen zur Abwehr einleiten, bevor der Hersteller eine offizielle Lösung bereitstellt. Parallel versetzt dies die Empfänger dieser Informationen in die Lage die Schwachstelle auszunutzen, bis das offizielle Update bereitsteht und installiert wurde. Genauso fordern Behörden oft den Zugriff auf den Source Code von Software für eine Analyse auf Schwachstellen. Die identifizierten Schwachstellen können sowohl bei der Bewertung von Sicherheitsrisiken als auch für Angriffe genutzt werden. Durch einen exklusiven Zugriff verschaffen sich die teilnehmenden Behörden einen Vorteil.

d) Faktor Mensch

Durch unzureichendes Sicherheitsbewußtsein der Mitarbeiter, in Kombination mit dem alltäglichen Stress kann ein Angreifer durch Social-Engineering-Angriffe an vertrauliche Informationen oder physikalischen Zugang kommen. Z.B. können Angreifer mittels Phishing Zugangsdaten erlangen oder als unbekannte „IT-Mitarbeiter“ Überwachungsgeräte installieren. Auch diese Angriffe fallen in der Regel nicht auf. Die wenigsten kennen alle IT-Mitarbeiter. Auch wird oft keine eindeutige „Legitimation“ oder „Identifikation“ der Unbekannten gefordert.

e) Erkennung

Im Rahmen unserer Arbeit führen wir sowohl verdeckte Penetrationstest (nur Geschäftsführer bzw. Oberbürgermeister, Datenschutzbeauftragter, Personalvertretung und ein eingeschränkter Personenkreis) als auch offene Penetrationstests (IT-Administratoren sind informiert). Bei verdeckten Analysen fallen wir in der Regel auch nach 1-2 Wochen nicht auf. Dabei gehen wir auf Grund eines begrenzten Auftrags noch relativ schnell und damit leicht zu erkennen vor. In den meisten Fällen werden Angriffe nicht erkannt. In einigen Fällen finden wir sogar während der Überprüfung Spuren von erfolgreichen Angriffen, welche sich über mehrere Monate erstrecken(teilweise solange die Protokoll-Dateien zurück reichen).

f) bekannter Fall

Mir ist ein Fall aus NRW bekannt bei dem über längeren Zeitraum über Schwachstellen in Web-Diensten der Stadt auf das interne Netzwerk der Stadt zugegriffen wurde, bei der auch staatlicher Eingriff vermutet wird. Man hatte sich über längeren Zeitraum Stück für Stück behutsam ins Netzwerk vorgetastet. Spuren lassen darauf schließen, dass versucht wurde auf die Infrastruktur von Bund und Ländern zuzugreifen. Die Täter konnten nicht identifiziert werden, man geht auf Grund des langen Durchführungszeitraums und des „professionellen" Vorgehen von einem Angriff durch einen Geheimdienst aus. Ob es sich hier tatsächlich um Angriffe eines Geheimdienstes handelt, kann man auf Grund des geringen Sicherheitsniveaus und der fehlenden Spuren nicht mehr sagen.

g) Motivation

Sowohl einige Geheimdienste wie auch Kriminelle fahren eine Strategie, bei der Sie alles speichern was Sie an Daten sammeln können. Wie interessant oder relevant die Daten sind wird in vielen Fällen erst später entschieden. Auch werden diese großen Datenmengen oft für Data-Mining und Profiling verwendet.

h) Daten

Gerade die Datenbanken der öffentlichen Verwaltung liefern dabei eine relativ gute Quelle, denn Sie verfügen über nahezu vollständige Datensammlungen zu allen Bürgern mit relativ geringer Fehlerquote. Z.B.

- elektronische Personen Register
- elektronisches Standesamt
- Ausländer-Datenverwaltung
- Listen für „Alias- Identitäten" (z.B. Zeugenschutz),

Dabei enthalten Datensammlungen teilweise sehr detaillierte Informationen über die Bürger. Insbesondere die Daten folgender Stellen können einen Aufschluß über die finanzielle Lage, Tätigkeiten, Lebensläufe, Gesundheit und sonstigen Probleme von Personen enthalten

- Jobcenter
- Jugendamt
- Schulamt(z.B. Schüler Leistungs-Daten)
- Sozialamt
- Ordnungsamt
- Finanzamt
- Betreuung und Verwaltung von Pflegebedürftigen und psychisch Kranken

Ein weiterer Aspekt der nicht verkannt werden sollte sind wirtschaftliche Interessen. Aus diversen Informationen können wirtschaftlich interessante Informationen hervorgehen:

- Stadtplanung
- Bauamt
- Gewerberegister
- Wirtschaftsförderungsanträge
- Ratsinformationssystem

Im Rahmen von Anschlägen können auch physikalische Schäden entstehen

- Manipulation von Alarmierungs- und Benachrichtigungssystemen bzw. andere Systeme der Einsatzleitstelle (z.B. Feuerwehr)
- Störung elektronische Meldestelle
- ggf. Zugriff auf kritische Infrastrukturen Strom, Wasser, Gas, Abwasser
  (bei Vernetzung mit Stadtwerken, ist teilweise eine direkte Steuerung einzelner Anlagen möglich)

Der Vollständigkeit halber sollte man darauf hinweisen, dass auch ein direkter finanzieller Vorteil möglich ist. Dieser ist allerdings in der Regel weniger im Fokus von Geheimdiensten als im Fokus normaler Krimineller. z.B. durch den Zugriff auf

- diverse Online-Banking-Lösungen
- Bußgeldstelle
- Haushalts, Kassen und Rechnungswesen
- Forderungsmanagement
- Pflege-Einstufungen
- diverse Vergütungsstellen

i) <u>Hinweise von Snowden</u>

Edward Snowden hat im Interview vom 26.01.2014 explizit nochmal darauf hingewiesen, dass es relativ unwahrscheinlich ist, dass die NSA nur Frau Merkel und nicht auch andere wichtige Persönlichkeiten bis hin zu kommunalen Politikern überwacht.

2. *Welche Maßnahmen sollte die Landesregierung kurz-, mittel- und langfristig ergreifen, um nordrhein-westfälische Behörden vor diesen und weiteren bekannt gewordenen Bedrohungen zu schützen? Könnten IT-Sicherheitsbeauftragte in den Behörden ein erster Schritt hin zu einer besseren Datensicherheit darstellen?*

a) <u>Grundprinzipien des Datenschutzes</u>

Bereits im Bundesdatenschutzgesetz (BDSG) sind die Grundlagen gelegt, welche in der heutigen Zeit immer mehr an Bedeutung gewinnen. Allerdings werden die Regelungen derzeit nicht wirksam durchgesetzt.

Insbesondere: **<u>§3a BDSG – Datensparsamkeit & Datenvermeidung</u>**

Es sollten Ausnahmen zurückgefahren werden und die Daten wo möglich reduziert werden. Auch sollte diese Regelung deutlich strikter durchgesetzt werden. Denn Daten nicht zu erheben ist der beste Schutz. Wo die Ausnahmen bestehen bleiben, müssen klare Rechtsvorschriften für einen effektiven Schutz geschaffen und durchgesetzt werden.

b) <u>Maßnahmen</u>

Die Maßnahmen weichen von Behörde zu Behörde und Kommune zu Kommune ab. Da auch ein unterschiedlicher Sicherheitsstatus herrscht.

Grundsätzlich sollte sofern es noch nicht passiert ist, eine Datenklassifizierung erfolgen, bei der die Brisanz der Daten und Systeme bestimmt wird. Besonders kritische Daten(z.B. Listen mit Personen aus Zeugenschutzprogrammen, Privatanschriften von gefährdeten Persönlichkeiten und deren Angehörigen) und Verfahren müssen ggf. bis eine „ausreichende“ Sicherheit gewährleistet werden kann wieder auf Papier oder auf dedizierte Systeme ohne Anbindung ans Intranet der Stadt umgestellt werden.
Daher sind im Rahmen der Sofort-Maßnahmen insbesondere einfache aber wirksame Maßnahmen umzusetzen und entsprechend vorhandene Verfahren und Systeme mittels bestehender Möglichkeiten abzusichern.

Danach sollte eine Sicherheitsstrategie mit entsprechender langfristiger Planung entwickelt werden. In diesem Rahmen sollten klare Kriterien für den Einsatz von Software bestimmt und vertraglich fest geschrieben werden. Beim aktuellen Sicherheitsstand werden viele Kommunen bereits viel Zeit benötigen sich vor „Gelegenheitshackern“ zu schützen.

Wirksame Maßnahmen, welche zum Schutz vor Geheimdiensten erforderlich sind, gibt es in vielen Fällen leider noch nicht. Möchte man auf lange Sicht auch die Geheimdienste aussperren, so muß man auf eine nahtlose Sicherheits-Kette hinarbeiten. Dies geht nur dann wenn eine exklusive „eigene Vertrauenskette“ aufgebaut werden kann, IT-Sicherheit von vorne herein bei Verfahren eingeplant wird, die Quellen der eingesetzten Software regelmäßig geprüft, alle Sicherheitsvorgaben eingehalten und die Produkte regelmäßig aktualisiert werden. Darüber hinaus müssen die Mitarbeiter für den bewußten Umgang mit der IT sensibilisiert werden.

c) Einsatz von Software

Oft werden blind teure Programme gekauft, um Sicherheit zu schaffen. In der Praxis bringt aber kein Programm von sich aus Sicherheit. Der Einsatz und die Konfiguration jeder Lösung müssen sicher konzipiert und implementiert sein. Wann sich der Kauf von Software lohnt, und wann eine reine Absicherung mit vorhandenen Mitteln reicht ist von der Situation abhängig.

Eines der typischen Beispiele sind so genannte Terminalserver (z.B. Citrix, Windows-Terminalserver) bei denen viele Benutzer zentral auf einem Server arbeiten. Dabei werden Eingaben an den Server geleitet und das Bild an den Benutzer übertragen. Durch das Arbeiten auf einem Server (in der Regel hinter jeglichen Schutzmaßnahmen) entstehen neue Risiken. Diese kann man absichern. In der Praxis erfolgt dies allerdings nur selten in ausreichendem Maß.

d) IT-Sicherheits-beauftragte

Teilweise existieren bereits „IT-Sicherheitsbeauftrage“ bzw. IT-Sicherheitsansprechpartner bei einigen Städten und kommunalen Dienstleistern. In der Praxis werden diese allerdings in wichtige Projekte nicht oder zu spät mit einbezogen. Auch haben Sie in der Regel keinen Einfluß.

IT-Sicherheitsbeauftragte sind nur dann ein Schritt in die erste Richtung, wenn sie:

- unabhängig sind
- genügend technische und organisatorische Grundkenntnisse besitzen um die Einschätzungen und Aussagen der Techniker und Fachverfahrensbetreuer einzuschätzen bzw. die richtigen Informationen zu fordern.
- Kontrollbefugnisse haben
- in alle Projekte aktiv und frühzeitig mit eingebunden werden

3. *Wie schätzen Sie die Gefahr der Verbreitung von Schadsoftware ein, wenn innerhalb von Behörden und in der Kommunikation zum Bürger mit einer Ende-zu-Ende Verschlüsselung gearbeitet wird? Wie gehen große Unternehmen mit diesem Thema um?*

Nutzung von Verschlüsselung

Gerade die Kommunikation mit öffentlichen Stellen enthält oft sehr sensible Daten. Daher ist der Verzicht auf eine Verschlüsselung als Grob-Fahrlässig anzusehen. Während die Stadt oder Kommune keinen direkten Einfluß auf die Verschlüsselung seitens der Bürger hat, so sollte Sie doch zumindest den Bürgern die Möglichkeiten bieten. Um keine Bürger auszugrenzen, sollten dabei alle gängigen Verfahren, so wie unabhängige Alternativ-Verfahren sofern möglich angeboten werden. Bei unverschlüsselter Kommunikation sollte immer auf einfache Möglichkeiten für eine gesicherte Kommunikation hingewiesen werden.

Gefahr durch Ende-zu-Ende-Verschlüsselung

In normalen Unternehmensnetzwerken werden Emails bei Eingang auf dem Server nach Viren, Spam oder gefährlichen Anhängen gescannt und gefiltert. Dabei muß man allerdings sagen, dass Virenscanner in der Regel nur bekannte Viren identifizieren. Es gibt zwar auch eine dynamische Erkennung auf Basis von „Viren-Merkmalen“, diese ist aber eher als schlecht einzuschätzen. Daher werden gezielte Viren, die speziell für einen Einsatz entwickelt wurden in der Regel nicht erkannt. Ende-zu-Ende verschlüsselte Emails kann dieser Filter nicht analysieren. Allerdings sollte auch auf jedem Endgerät eine aktuelle Antiviren Software installiert sein. Diese filtert sofern der gleiche Hersteller eingesetzt wird, die gleichen Viren. Bei unterschiedlichen Antiviren-Herstellern hätte man mit einem doppelten Scan eine leicht höhere Erfolgsquote, welche aber nur einen geringen Sicherheitsgewinn bietet. Es ist ebenfalls möglich mittels entsprechender Regeln unsichere Anhänge auf den Endgeräten zu blockieren. Daher es kann ein ähnlicher Schadsoftware-Schutz für Ende-zu-Ende-Verschlüsselte Emails, wie auch für unverschlüsselte Mails genutzt werden.

Die primären Probleme bestehen dann eher im Organisatorischen/Rechtlichen. So ist es Beispielsweise erforderlich, dass amtliche Unterlagen archiviert werden müssen. Bei einer Ende-zu-Ende-Verschlüsselung muß in diesem Fall ebenfalls sichergestellt sein, dass die Schlüssel entsprechend gesichert werden.

Zu dem ist es so, dass Personen erkranken oder ausscheiden. In diesem Fall müßten die Nachfolger bzw. Vertreter Zugriff auf die Post haben. Bei einer personalisierten Ende-zu-Ende Kommunikation müssen auch diese Fälle betrachtet werden.

Aber das sind durchaus keine unlösbaren Probleme. Es ist lediglich wichtig, dass die Anforderungen klar definiert werden und alle Fälle berücksichtigt werden. Die Anforderungen können von Szenario zu Szenario abweichen. Wenn eine betreute Person z.B. einer vertrauten Person beim Jugendamt sich offenbaren will oder bei einer strategischen Kommunikation zwischen den Stadträten ist ggf. eine echte Ende-zu-Ende Kommunikation sinnvoll. Diese ist persönlich. Bei normaler Amtskommunikation ist eher ein Gruppen-Modell (ein gemeinsamer Schlüssel für mehrere Personen aus einem Fachbereich, der z.B. auch auf einer Webseite abrufbar ist) sinnvoll, bei dem auch Vertreter und Nachfolger auf die Kommunikation zugreifen können.

Sicherheit von Ende-zu-Ende-Verschlüsselung

Zu beachten ist, dass auch bei einer Ende-zu-Ende-Verschlüsselung neugierige Administratoren in vielen Fällen direkt unbemerkt von außen auf die Systeme der Betroffenen zugreifen können und sich so Zugriff auf Schlüssel und Inhalte von Mails verschaffen können.

Gängige Ende zu Ende-Verschlüsselungsverfahren verschlüsseln in der Regel nur Inhalte, nicht aber Meta-Daten (z.B. Titel, Absender und Empfänger). Um solche und andere Einschränkungen zu verstehen, müssen evtl. Schulungen durchgeführt werden.

Auch darf eine Verschlüsselung nicht als 100% sicher betrachtet werden. Laut Edward Snowden ist zwar die NSA noch nicht soweit, allerdings sind auch diese Informationen bereits veraltet. Es gibt bereits Quanten-Algorithmen, die zum knacken üblicher aktueller „Verschlüsselungsverfahren“ genutzt werden können. 2001 wurde das Verfahren mit 7 Qubits nachgewiesen. Für reale Schlüssellängen benötigt man das Quanten-Rechner mit ca. 150-300 Mal so vielen Qubits. Derzeit lassen sich nach öffentlichen Erkenntnissen noch keine Quanten-Computer mit ausreichend Qubits und den richtigen Funktionalitäten bauen.

Durch das Speichern von verschlüsselten Daten, können diese allerdings auch rückwirkend entschlüsselt werden.

Umgang von Firmen mit Verschlüsselung

Es gibt verschiedene Modelle:

1) Verschlüsselung wird untersagt (Man möchte sich nicht mit den daraus resultierenden Herausforderungen beschäftigen)

2) Bei verschlüsselten Mails wird auf das Endgerät vertraut. Der zentrale Scan entfällt dann.

3) Es werden Gruppen-Accounts statt personalisierten Email-Adressen eingesetzt. Ein Scan erfolgt hier ebenfalls nur auf dem Endgerät.

4) Die Verschlüsselung erfolgt zu einem zentralen Verschlüsselungssystem der Firma. Die Mails werden dort entschlüsselt und auf Viren gescannt. In einigen Fällen werden die Mails dann für die interne Zustellung neu verschlüsselt. In diesem Fall hätten Administratoren auf dem System Zugriff auf alle Mails.

Eine unverschlüsselte Kommunikation insb. vertraulicher Daten wie sie im kommunalen Umfeld übertragen werden ist m.E. unverantwortlich. Fehlende Möglichkeiten sorgen in der Regel dafür, dass unverschlüsselt höchst sensible Daten per Email oder Cloud-Diensten übermittelt werden.

4. *Die behördliche IT-Landschaft in NRW ist auf kommunaler, regionaler und landesweiter Ebene sowie zu Bundesbehörden vielfach miteinander vernetzt. Ist zur Absicherung der Netze eher eine zentrale, oder eine dezentrale Struktur sinnvoll? Befürworten Sie eine Angleichung der verschiedenen IT-Systeme (z.B. der Ratsinformationssysteme) oder sollte die Fragmentierung bewahrt bleiben?*

a) Aktuelle Lage

Viele Kommunen sind direkt oder indirekt an das Behördennetzwerk angeschlossen. Sie sind allerdings ebenfalls im Rahmen von Partnerschaften auch mit anderen Kommunen oder kommunalen Dienstleistern direkt verbunden. Für über das Internet bereitgestellte Dienste und Webseiten besteht oft ein direkter Internet-Zugang. Auch gibt es in einigen Kommunen öffentlich zugängliche Terminals für Bürger, die direkt mit dem Intranet der Kommune verbunden sind. Damit ist der Zugriff auf das Netzwerk von vielen Kommunen möglich. Von dort aus besteht oft einfacher Zugriff auf andere Kommunen, sowie Landes- oder Bundesverfahren.

b) Anpassung

Dafür ist eine große zentrale Anwendung weniger flexibel auf die regionalen Bedürfnisse anpaßbar. Durch eine nicht optimierte Anwendung, erhöht sich der Aufwand für die Sachbearbeiter. Dadurch werden Kosten vom Betrieb der Anwendung auf das Personal verschoben.

c) Wartung

Auch fällt es oft schwer Auszeiten und andere Wartungstätigkeiten abzustimmen. Was dazu führt, dass oft wichtige Aktualisierungen nicht oder nicht zeitnah eingespielt werden und Sicherheitslücken offen bleiben.

d) Störungen

Eine Störung oder ein Ausfall der zentralen Lösung, führt in der Regel bereits in kurzer Zeit zu hohen Kosten (z.B. durch Arbeitsausfall oder nicht eingehaltene Fristen).

e) Sicherheit

Egal wie sicher ein System aufgebaut ist, es wird immer technische Schwachstellen geben, die einen Zugriff auf die Daten ermöglichen oder Personen die Zugriff auf die Systeme haben. Ein Angreifer braucht nur einmal eine Schwachstelle zu identifizieren um auf alle Daten zuzugreifen zu können. Bei vielen unterschiedlichen Systemen hingegen muß ein Angreifer deutlich mehr Aufwand aufbringen und gelangt trotzdem an deutlich weniger Daten. Bei jedem Einzelangriff besteht die Gefahr, dass er entdeckt wird und Maßnahmen eingeleitet werden.

f) Mißbrauch

Auch wenn die technischen Schwachstellen geschlossen sind. Gibt es immer Personen die darauf zugreifen können. So kenne ich persönlich diverse Fälle, wo Mitarbeiter im öffentlichen Dienst ihre Stellung dazu mißbrauchen z.B. Bußgeldbescheide zu löschen oder Recherchen über den Nachbarn oder die Ex-Frau anzustellen.

g) Social Engineering

Darüber hinaus kann auch unvorsichtiges Verhalten auf Grund von Unwissen, Nachlässigkeit und Stress von Angreifern ausgenutzt werden. Laut dem Verfassungsschutz wird beispielsweise auch nach den Zeiten des kalten Kriegs mit Methoden wie Bestechung, Verführung und Erpressung gearbeitet um Schlüssel-Personen zu Kontrollieren und vertrauliche Informationen zu gewinnen. Selbst mit weniger drastischen Mitteln ist es möglich sich von gutgläubigen Beamten gesicherte Räume aufschließen zu lassen und so Überwachungssysteme zu installieren, das Netzwerk oder Telefon auszuleiten oder Informationen zu stehlen. Diese Angriffe funktionieren bei ungeschultem Personal in fast allen Fällen.

h) Monopol-Stellung

Derzeit sind einzelne Anbieter auf dem Markt, die bestimmte Produkte anbieten, welche bekannte Schwachstellen haben. Trotzdem bieten viele Anbieter entweder „Sicherheits-Updates“ gar nicht, nur gegen exorbitant hohe Beträge oder erst sehr spät an. Auf Grund der Monopol-Stellung besteht kein Wettbewerb oder anderes Druckmittel gegen den Hersteller.

i) historische Entwicklung

Schaut man sich die historische Gestaltung der Gesetzgebung an, so wurden insbesondere aus den nach dem 2. Weltkrieg gewonnen Erkenntnissen an vielen Stellen dezentrale Speicherungen und Verarbeitungen vorgeschrieben, um eine zu starke Bündelung von Macht und den damit möglichen Mißbrauch zu verhindern. Durch die zunehmende Zentralisierung entsteht hier ein Paradigmen-Wechsel.

j) Praxis

Im Rahmen unserer Sicherheits-Überprüfungen hat sich herausgestellt, dass gerade kleine Kommunen oft besser aufgestellt sind. Allerdings sind in diesen Fällen oft Verfahren an kommunale IT-Dienstleister ausgelagert. Diese IT-Dienstleister unterliegen meistens einem harten Preiskampf, der sich deutlich in der fehlenden IT-Sicherheit bemerkbar macht.

5. *Welche Elemente sollte ein Datenschutzprogramm für die Kommunen beinhalten?*
   a) Alle Mitarbeiter im öffentlichen Dienst sollten für den Umgang mit sensiblen Daten geschult werden. Empfehlenswert wäre hier eine Initiale Veranstaltung bei der grob die Bedeutung der Daten erklärt wird, gezeigt wird was möglich ist und wie man sich davor schützt. Sowie ein Konzept zur regelmäßigen Auffrischung der Kenntnisse und zur Schärfung der Sinne.
   b) Es müssen klare organisatorische Regelungen geschaffen werden.
   c) Es müssen technische Grundvorgaben geschaffen werden. Ausnahmen dazu sollten nur temporär, mit Begründung und Risikobewertung möglich sein.
   d) Es müssen regelmäßig sowohl technische als organisatorische Stichproben erfolgen. Dabei sollte nie der einzelne Mitarbeiter sondern immer das Sicherheitsziel im Fokus stehen.
   e) Für Bereiche mit besonders hohem Schutzniveau müssen erweiterte Schulungsmaßnahmen und Vorgaben erfolgen.

6. Wie beurteilen Sie mögliche Kosten der Maßnahmen zur Stärkung der IT-Sicherheit im Verhältnis zu möglichen Schäden durch Datenmissbrauch, Datenverlust oder Datendiebstahl? Wie beurteilen Sie in diesem Zusammenhang möglichen Mehraufwand in der täglichen Arbeit für Mitarbeiter. Kann sich NRW angemessene IT-Sicherheitsstandards und verschlüsselte Kommunikation leisten?

   Die richtige Frage muß lauten: Kann es sich NRW leisten auf **effektive** IT-Sicherheitsstandards zu verzichten?

Beispiele:

   a) Daten sind die Ware der Zukunft, ein wirksamer Schutz dieser Daten ist daher unerläßlich.
   b) Der Staat ist verpflichtet die Grundrechte der Bürger zu schützen. Das Bundesverfassungs-Gericht hat bereits in mehreren Fällen auf die Pflicht des Staates hingewiesen, in seinem Namen oder auf seine Anweisung erhobene Daten schützen zu müssen.
   c) Ein besonderer Schutz ist insbesondere bei den für die öffentliche Verwaltung erhobenen Daten geboten. Diese sind oft besonders sensibel und der Bürger kann dieser Datenverarbeitung in der Regel nicht widersprechen.
   d) Diverse Informationen (Bauvorhaben, Antrage, Nachweise zur Steuererklärung, …) bieten Anhaltspunkte über wirtschaftliche Vorhaben. Daraus lassen sich gezielt Informationen ableiten und ausländische Firmen können so wirtschaftliche Vorteile erlangen.
   e) Insider-Informationen können Wettbewerbsvorteile schaffen.
   f) Persönliche Informationen die durch diverse Stellen z.B. Sozialamt, Job-Center, Jugendbetreuung oder andere Stellen gesammelt werden, können dazu genutzt werden Personen zu diskreditieren.
   g) Detaillierte Schüler-Leistungsdaten, wie sie im Rahmen der Qualitätssicherung gesammelt werden, sind für viele potentielle Arbeitgeber interessant.

   h) Das bekanntwerden von Daten wie z.B. Aufenthaltsorte und Identitäten von gefährdeten Persönlichkeiten (z.B. Zeugenschutz, verdeckte Ermittler, Richter, …) kann zur Gefahr für Leib und Leben werden. Insbesondere sind oft auch die Angehörigen von Entscheidern und Reichen der Gefahr der Entführung oder Erpressung ausgesetzt.
   i) Auch detaillierte Informationen über alle Ausländer sind für Rechtsradikale-Gruppen, ihre Propaganda und kriminellen Tätigkeiten interessant.
   j) Im Falle von Stadtwerken kann auch ein Angriff auf kritische Infrastrukturen (Strom, Wasser, Gas) erfolgen. Diese können unter Umständen bleibende Umwelt-Schäden herbeiführen.
   k) Auch eine gezielte Manipulation von zentralen „Koordinationssystemen“(z.B. Notruf, Einsatzleitsystem) von Feuerwehr oder Polizei im Rahmen eines Anschlages oder einer Katastrophe können Leben gefährden.

l) Aktuell ist auch ein Zugriff auf die Konten der Stadt in vielen Fällen möglich. Dadurch können finanzielle Schäden entstehen, die auf Grund des fahrlässigen Umgangs vermutlich nicht von einer Versicherung gedeckt sind.

Man hat in den letzten Jahren bzw. Jahrzehnten viele Verfahren auf den Einsatz von Computern umgestellt. Dabei wurde allerdings in vielen Fällen die IT-Sicherheit, wenn überhaupt nur unzureichend betrachtet. Diese Versäumnisse von Jahrzehnten, wird man nicht auf einen Schlag abschalten können. Auch muß man neu rechnen, welche Verfahren mit hohem Risiko unter Berücksichtigung von wirksamen Maßnahmen überhaupt noch Online durchgeführt werden sollten und wie rentabel dies ist. Ggf. müssen einzelne besonders sensible Verfahren(z.B. mit Gefahr für Leib und Leben), zumindest bis ein ausreichender Schutz gewährleistet werden kann zeitweise zurück auf Papier oder dedizierte Systeme ohne Netzanbindung umgestellt werden.

7. *Wie bewerten Sie die bestehenden Bildungsmaßnahmen im Bereich Medien-, Computersicherheit- und Datenschutzkompetenz und welche edukativen Maßnahmen sollte das Land Ihrer Meinung nach fördern? Welche Priorisierung sollte stattfinden, welchen Umfang sollten diese Maßnahmen haben und welche Zielgruppen sind dabei von größter Wichtigkeit? Welche edukativen Maßnahmen sollten in den Behörden ergriffen werden?*

a) <u>Bildung der Mitarbeiter im öffentlichen Dienst</u>

Die Lage ist derzeit unzureichend, viele Mitarbeiter kennen weder die Bedeutung noch die Risiken der Daten, mit denen Sie umgehen. Fremde werden nicht geprüft, Gäste werden mit IT-Equipment allein gelassen.

Hier wäre die Schulung siehe Antwort zu 5) sinnvoll.

b) <u>Schulische Bildung</u>

Zum Inhalt des aktuellen Lehrplan kann ich relativ wenig sagen. Ich empfehle allerdings die folgenden Themen in geeigneter Form in den Lehrplan für alle Schüler aufzunehmen. Wichtig ist es dabei auch die Lehrer fortzubilden:

- Medienkompetenz
  Insbesondere das Bewerten und Filtern von Informationen nach Quelle, Intention und Qualität wird immer wichtiger. Es stehen viele Informationen und Inhalte bereit, von denen viele sehr wertvoll sein können, aber einige auch nicht unreflektiert betrachtet werden sollten. Wirksame Filter sind derzeit nicht möglich. Gerade die am meisten gefährdeten Altersgruppen sind oft in der Lage diese Filter einfach zu umgehen, aber können diese Inhalte noch nicht reflektieren. Daher sollte jeder der im Internet surft in der Lage sein, für sich selbst zu identifizieren, wie vertrauenswürdig Quellen sind, wie schlüssig Sachverhalte sind und wie man Propaganda identifizieren kann. Auch sollte darüber aufgeklärt werden, welche Folgen eine Veröffentlichung von sensiblen Informationen über einen selbst oder andere haben kann und wie man daraus einen bewußten Umgang mit den Medien ableiten kann. Auch sollte jeder über die Grundkenntnisse für eine aufmerksame und sichere Nutzung verfügen.

- IT-Sicherheit
  Grundkenntnisse der IT-Sicherheit sind sicherlich hilfreich. Aber für den normalen Schüler sollte man sich hier auf die Grundlegenden Themen beschränken:
  - aufpassen mit verdächtigen Anhängen
  - unbegründetes Leuchten der „Status-LED“ der Kamera

  - Bei normaler Email ist weder Absender noch Inhalt gesichert
  - Umgang mit Paßwörtern

- Jugendschutz
  Auch müssen die Kinder darauf hingewiesen werden, wie Sie mit Fremden im Netz umzugehen haben, was ok ist und was sie besser den Eltern oder Lehrern melden sollten.

- Datenschutz
  Neben den Grundprinzipien des Datenschutz (z.B. Datensparsamkeit und Datenvermeidung) sollten hier auch die möglichen Folgen für die einzelne Person und die gesellschaftlichen Auswirkungen von Überwachung behandelt werden.

c) <u>Wissen für die Bevölkerung</u>
Das BSI bietet mit der Webseite http://www.bsi-fuer-buerger.de bereits zahlreiche vereinfachte Informationen an. Hier wäre eine Bewerbung und Ergänzung sinnvoll.

Betreff: Whistleblowing und PRISM - Anhörung A09 - 06.02.2014

zum Antrag „Whistleblowing — eine Form von Zivilcourage, die unterstützt und geschützt werden muss" (Dr. 16/3437)

Zum 2. Themen-Komplex kann ich nur einige allgemeine Aussagen treffen:

Der Gesetzgeber sollte, wenn bestimmte Kriterien eingehalten werden einen rechtlichen Schutz zusichern. Grundsätzlich könnte eine unabhängige Stelle eingerichtet werden, welche auch anonyme Hinweise ermöglicht. Allerdings kann dies aus meiner Sicht nur eine Option unter vielen sein, die nicht alle Fälle abdeckt.

Solche Kriterien könnten z.B. sein:

- keine Bagatelldelikte
- es sollte ein öffentliches Interesse bestehen
- falls möglich keine Gefährdung von Personen
  (Das Beispiel Snowden zeigt, in vielen Fällen müssen keine Namen oder konkreten Aktionen genannt werden, es reichen allgemeine Sachverhalte)

Je nachdem wen die Hinweise betreffen und wie die Umstände sind, kann es erforderlich sein, dass ein gewisser Sachverstand erforderlich ist. Auch muss ein Hinweisgeber eine Vertrauensbasis zur geeigneten Stelle aufbauen, um sensible Informationen weiter zu geben.

Zentrale Hinweisgebersysteme können leicht überwacht werden und sind somit je nachdem wer betroffen ist nicht als sicher anzusehen. Auch interne Hinweisgebersysteme bieten keinen ausreichenden Schutz.

Abhängig vom Inhalt kann es sein, dass durch den Inhalt die Quelle preisgegeben wird. Dann ist eine anonyme Möglichkeit nicht mehr gegeben.

Die Gefahr des Denunziantentums besteht immer. Hier sollte man eine Bagatellklausel einbauen. Ein starker Schutz und eine Würdigung ist angemessen. Eine größere Entlohnung fördert Denunziantentum. Eine öffentliche Belobigung kann abhängig von der Situation zu Nachteilen für den Hinweisgeber führen.
Um vor Falschaussagen zu schützen sollten wissentliche Falschaussagen ähnlich wie vor Gericht unter Strafe gestellt werden. Veröffentlichen Stellen, sollten soweit möglich die Echtheit der Angaben prüfen und im Zweifel auf eine Veröffentlichung verzichten oder zumindest auf die „fehlende“ Prüfbarkeit hinweisen.

Kündigungsschutz und Maßregelungsverbot funktionieren soweit ich das Beobachten konnte in erster Linie in größeren Betrieben mit starker Personal-Vertretung. Bei kleineren Betrieben, findet man in der Regel andere Gründe um den Kündigungsschutz oder das Maßregelungsverbot zu umgehen.

Compliance-Maßnahmen werden primär von internationalen Unternehmen betrieben, welche direkt oder indirekt dem US-Recht (z.B. Sarbanes-Oxley Act - SOX) unterliegen. Da fehlende Compliance zu Existenz bedrohenden Strafen wie z.B. dem Ausschluß vom Handel in den USA oder mit US-Firmen führen kann. Ansonsten ist das Thema Compliance in Deutschland nur bedingt angekommen.