
DATENSCHUTZ

Grundlagen über die Bedrohungen im Bereich des Internets und der Telekommunikation

Schlussfolgerungen für ein verantwortliches Handeln nach der Bewertung der Sicherheit vorhandener und einzuführender ganzheitlicher Netzwerkkonzepte innerhalb der kommunalen Verwaltung und der daran angeschlossenen Dienstleistungsunternehmen.

Autor:

Kurt Klein

Juli 2015

Index

Einführung

Während der Einarbeitung in den Themenkomplex eines sachgebietsübergreifenden Computernetzwerkes der Stadt Duisburg und der darüber notwendigen Abstimmung innerhalb der Ratsfraktion PIRATEN-SGU-BL (PSL) wurde offensichtlich, dass die überwiegende Mehrheit zwar ein Unwohlsein gegenüber der allgemeinen technischen und gesellschaftlichen Entwicklung digitaler Technik empfindet, sich aber gleichwohl auf Grund der vermeintlichen Komplexität des Themas, als hilfloser Spielball eben dieser Prozesse betrachtet. Dies verführt die meisten Menschen reflexhaft, sich Dingen zu widmen, bei denen man eine Chance sieht sie auch beeinflussen zu können.

Dies ist insofern problematisch, als das man sich dem Einfluss dieser Technik und deren Anwendung nicht entziehen kann. Daher ist es wünschenswert, dass gerade die Politik zuverlässige Rahmen-bedingungen für den Einsatz von Informationstechnologien vorgibt und sie nicht durch monopolisierte, wirtschaftliche Interessen aufgezwungen werden.

Daher ist diese Abhandlung dahingehend zu verstehen, dem Laien eine Übersicht über derzeitigen technische Möglichkeiten und der tatsächlich stattfindenden Anwendung derselben für unerwünschte Zwecke einzuschätzen. Daher mag es bei einigen Punkten den Jüngern der reinen Lehre an einer gewissen Trennschärfe fehlen, insgesamt halte ich es bei einer Übersicht allerdings auch nicht für zielführend, den Begriff des Hackers in 200 Unterkategorien aus zu definieren, dann liest es nämlich keiner mehr.

Denkansätze

Was kann man im Bereich des Datenschutzes also noch bewegen? Eigentlich eine Menge, wenn man mal die Worthülsen beiseite schiebt, mit denen wir unablässig überschüttet werden.

Erster logischer Fehler in der Argumentationskette neoliberaler Politik ist, dass private Anbieter es immer besser können. Eine effiziente öffentliche Verwaltung, deren Personal nach fachlicher Qualifikation und charakterlicher Eignung ausgewählt wurde, welches konsequent aus-, weiter- und fortgebildet wird, kann zum Teil bessere Dienstleistungen erbringen.

Insbesondere die nicht quantifizierbaren Mehrwerte wie Integrität, Orientierung am Gemeinwohl unabhängig von Parteien und der Verpflichtung, der auf die im Grundgesetz bindend festgelegten Normen, kann kein privater Dienstleister konkurrenzfähig anbieten.

Von den meisten unbemerkt steht Politik auf allen Ebenen nun vor einem Scheideweg. Wer die Versorgungsnetzwerke kontrolliert, kontrolliert den gesellschaftlichen Wandel, beziehungsweise kann gleiche Ausgangsbedingungen für alle garantieren. Entweder setzt Politik hier klare Rahmenbedingungen oder sie macht sich auf unabsehbare Zeit irrelevant. Daher kann auch für die kommunale Politik nur gelten:

> ***Erste Priorität haben die Umsetzung von Post- und Telekommunikationsgesetz, so wie das Bundes- und Landesdatenschutzgesetz NRW.***

Um dies zu garantieren, müssen die Kernbereiche und Netzwerke definiert werden, welche der alleinigen Kontrolle der öffentlichen Hand unterliegen und in welchem Umfang diese ausfallsicher zu funktionieren haben. Diese sind unbedingt in eigener Regie der Verwaltung aufzubauen und zu betreiben. Im Rahmen finanzieller Zwänge würde es sich hier anbieten, regionale Zweckverbände mit

benachbarten Kommunen zu gründen, da eine vernetzte Verwaltung hier große Einsparpotentiale bietet.

Mess-, Regel- und Steuerkreise in kritischen Infrastrukturen (Frisch- und Abwasser, Energie, Telekommunikation, Verkehrsinfrastruktur und anderen) sind zwingend physikalisch (kein kabel- oder funk-gestützter Zugang) vom Internet zu trennen. Da die entsprechenden Betreiber hier zukünftig durch den Bund immer mehr in die Pflicht genommen werden, liegt der Einspareffekt in einem durchdachten Gesamtkonzept darin, dass nicht mit neuen gesetzlichen Auflagen teure Nachinvestitionen zu tätigen sind. Einer der Faktoren, der private Anbieter auf mittelfristige Sicht immer teuerer macht als Eigenleistungen ist der, dass sie sich jede Änderung teuer bezahlen lassen.

Ist-Zustand

Die IT-Anwendungen der Stadt Duisburg (und ich schreibe hier sehr bewusst nicht Konzern!) sind im Laufe der letzten 20 Jahre gewachsen. Es wurden Lösungen beschafft und betrieben, die auf den einzelnen Einsatzzweck zugeschnitten waren. Dies zeitigt heute naturgemäß eine Unverträglichkeit der verschiedenen Datenhaltungen und Schwierigkeiten bei dem Austausch und der Nutzung dieser Daten.

Es ist somit tatsächlich an der Zeit und wünschenswert einen sachgebietsübergreifenden Gesamtansatz zu wählen. Insgesamt besteht hier ein hohes Potential an Effizienzgewinn und finanzieller Einsparungen. Gleichzeitig ermöglicht ein erfolgreiches Eindringen in diese Datenbestände, dann aber auch ein Schadenspotential, welches ungleich größer ist, als die Gefahren durch die derzeit existierenden Systeme.

Für einen allumfassenden Datenzugriff muss ein Angreifer derzeit eine Vielzahl von Insellösungen kompromittieren, bevor er alle Daten zusammen fahren kann. Daher ist ein stringenter systemisch angelegter Datenschutz kein Thema für Sektierer, sondern existentielle Grundlage für die Schaffung einer allumfassenden Lösung. Hier insbesondere in Abgrenzung an die private Wirtschaft, als Teil der staatlichen Verwaltung unserer Gesellschaft.

Datenschutz, dass unbeliebte Thema

Mit der Drucksache 15-0015 befindet sich ein Konzept der Duisburger Kernverwaltung im Umlauf, dem ich schwerste konzeptionelle Defizite unterstelle. Während der Ausschusssitzung am 12.06.2015 wurden aus den eigentlich geplanten 16 Fragen exemplarisch vier gestellt. Die Beantwortung durch die Kernverwaltung bestärken mich eher in dem Verdacht, dass gewisse existentielle Investitionen in die personelle, organisatorische und bauliche Absicherung unterbleiben werden.

Auch nach Edward Snowden ist das allgemeine Sicherheits-bewusstsein eher schwach ausgeprägt, da sich den meisten Menschen nicht erschließt, in welchem Umfang die digitale Welt sie bereits betrifft. Vor allem ein falsches Sicherheitsempfinden, insbesondere bei jenen, die meinen wenig bis gar nicht betroffen zu sein, könnte dies zu einem wirklich bösen Erwachen führen.

Auch wer das Internet nur zu Recherchezwecken zu nutzen meint und sich dem digitalen Fortschritt ansonsten verweigert, überlässt den Suchmaschinenbetreibern und der privaten Werbeindustrie einen solchen Datenbestand, dass erschreckend umfangreiche Persönlich-keitsprofile zusammengestellt werden (können).

"*Google kennt dich besser als du selbst*" ist keine leere Floskel!

Alles wird gespeichert und steht den amerikanischen Nachrichten-diensten ohne Richtervorbehalt zur Verfügung. Wenn ein Such-kriterium einen als „interessante Person“ auswirft, werden in einem zweiten Schritt die Daten aus sozialen Netzwerken (Facebook, Twitter und Konsorten), Bankdaten und Kommunikationsdaten (Stichwort Vorratsdatenspeicherung (VDS) und Bestandsdaten-auskunft (BDA)) herangezogen und eingearbeitet. Sofern letzteres aus deutschen Datenbeständen stammt, muss Homeland Security noch ein Amtshilfeersuchen mit dem Schlüsselbegriff Terrorismus stellen und wird dann bedient.

Bei diversen Abkommen wie SWIFT geschieht das bei den Bankdaten und Bankverkehrsdaten automatisch.

> Insgesamt ist es also weniger eine Frage was ich zu verbergen habe, sondern eher, wie diese Daten von Dritten zusammengestellt und interpretiert werden!

So kann man sich sehr schnell von einem eher mäßig witzigen Facebook-Nutzer zu einem Terrorverdächtigen mit Einreiseverbot wandeln, wie ein australischer Tourist zu seinem Leidwesen letztens erst erfahren musste. In solchen Fällen mag man eher den Kopf schütteln, in anderen Teilen der Welt werden Menschen auf Grund solcher Datencollagen und einem folgenden Verfahren, das jeglichen rechtsstaatlichen Standards Hohn spricht, in ihren Häusern mit Raketen beschossen.

Ein zweiter Aspekt den man hier nicht außer Acht lassen sollte: Es mag sein, dass ich nichts zu verbergen habe, wer aber voll-umfänglichen Lesezugriff besitzt, kann in den meisten Fällen auch Daten schreiben.

Kommt nicht vor?

Kanada hat mit der Gesetzesvorlage C-51 dieses Jahr noch einmal deutlich die Gangart verschärft. Der Geheimdienst wird ausdrücklich autorisiert, gegen Terrorismusverdächtige im In- und Ausland vorzugehen. Mord und Beschädigung der sexuellen Integrität sind ausgeschlossen, ansonsten ist alles erlaubt was die Kreativität der Mitarbeiter hergibt. Spätestens jetzt sollte jeder kurz in sich gehen, ob er vielleicht mal bei Facebook oder Twitter den falschen Eintrag mit *gefällt mir* markiert oder weitergeleitet hat, denn auch Unterstützer machen sich strafbar. Die Definition, was Unterstützung von Terror ist, obliegt weites gehend der Einschätzung des Mitarbeiters und ein rechtsstaatliches Verfahren zum Schutz der Beschuldigten ist ausdrücklich ausgeschlossen.

Da wir Deutschen ja in den letzten 200 Jahren nur ausnehmend gute Erfahrungen mit der Staatsgewalt hatten, möge nun jeder selber entscheiden, ob es eine gute Idee ist, möglichst viele Bereiche des privaten Lebens ohne jeglichen Anfangsverdacht dem unkontrollierten Zugriff der Staatsgewalt auszuliefern. Einer Staatsgewalt übrigens, bei der Menschen wie Du und Ich arbeiten, mit all ihren Stärken und Schwächen, wie man regelmäßig der Berichterstattung in den Medien entnehmen kann.

In der Folge befassen wir uns mit den anderen Spielern auf dem Feld. Diese kann man recht gut in drei verschiedene Gruppen einteilen.

Der Amateur: Dessen Ziele, Methoden und Vorgehensweisen sich aus den unterschiedlichsten Motivationen ergeben können. Hier ist auch der klassische Begriff des Hackers einzuordnen.

Der Kriminelle: Mittlerweile ein Multimilliarden Euro-Markt, der daher auch entsprechende Vergütungen an Spitzenprogrammierer oder Innentäter zahlen kann. Hier werden bei entsprechenden Gewinnerwartungen mittlerweile auch der Aufwand an Zeit, Geld und Personal nicht gescheut, die für flankierende Maßnahmen außerhalb des Cyberspace anfallen.

Der staatliche Akteur: Befasst sich sowohl mit Angriff als auch Verteidigung im Informationsraum, je nachdem welchen Auftrag er gerade hat. Hier sind die meisten der so genannten „qualifizierten Attacken“ anzusiedeln. Damit ist gemeint, dass die Mails, welche den Schadcode enthalten, meist so gestaltet sind, dass der Empfänger davon ausgeht, den Absender zu kennen und ihm deswegen trauen zu können (vgl. Schadmail im Bundestag). Hier werden im Umfeld des Zieles und lange vor der Attacke entsprechende Daten gesammelt. Ziel ist hierbei meist auch nicht Schaden im Betrieb zu erzeugen, sondern möglichst viele Informationen unentdeckt zu sammeln. Zweites Ziel ist häufig auch möglichst tief in ein System einzudringen, um dann alle entsprechenden Optionen für einen Angriff oder eine Sabotage parat zu haben.

Der Übergang zwischen diesen drei Akteuren ist nicht scharf abgegrenzt und meist fließend. So kann der ehemals jugendliche Hacker durchaus später nach einer entsprechenden Ausbildung im Staatsdienst wiederzufinden sein. Kriminelle können bei einem selbstständigen Programmierer entsprechende Dienstleistungen einkaufen. Die gefährlichste Variante des Akteurs ist derjenige, der nachdem er Zugriff auf staatliche Ressourcen hatte seine Kenntnisse und ggfs. entsprechend hochwertige Programme für kriminelle Zwecke zur Verfügung stellt.

Der Amateur

Hierbei handelt es sich meist um spätpubertierende junge Männer, die ihre Fähigkeiten als Programmierer üben oder sich in entsprechenden Gruppen profilieren wollen. Gängige Werkzugkästen zum Zusammenklicken von Schadprogrammen gibt es auf einschlägigen Seiten für jeden Bedarf und für jeden Geldbeutel zum herunterladen. Der Schaden ist meist örtlich begrenzt, was allerdings meistens auch den eher übersichtlichen Programmier- und Systemkenntnissen dieser Personengruppe zuzuschreiben ist. Die Fähigeren unter ihnen finden sich häufig später in einer der anderen Gruppen wieder.

Das wohl prominenteste Beispiel war 2003 der groß aufgemachte Fang des Programmierers einer MSBlaster-Variante, einem Computer -wurm der XP und Win2000 Systeme angriff und zum Absturz brachte. Der nämliche Programmierer hatte allerdings verschiedene Wurmschnippsel eher stümperhaft in Word zusammengeschustert. Der eigentliche Programmierer von MSBlaster ist bis heute unbekannt. Ich führe dies deshalb hier auf, da es ein pikantes Detail dazu gibt. Der 18 jährige konnte nur deswegen überführt werden, da er in mindestens einem Fall eine Word-Datei mit dem Schadcode verschickt haben musste. Seitdem sollte jedem Nutzer des Office Paketes bewusst sein, dass mindestens folgende Informationen als Metadaten in Office Dokumenten gespeichert werden:

Angemeldeter Computernutzer, Computerkonfiguration mit Seriennummern und MAC-Adressen.
(Machine Access Code = Fingerabdruck digitaler Schaltkreise)

Diese Metadaten wurden dazu benutzt, den Rechner der Ursprungs-datei zu identifizieren. Inwieweit weitere Daten aus diversen Protokoll-dateien gespeichert werden, ist unbekannt. Microsoft ist bis heute eine Erklärung schuldig, zu welchem Zweck diese Daten gespeichert und mit jedem Dokument auch übermittelt werden.

Der Kriminelle

Auch hier finden sich unterschiedliche Motivationen. Während die meisten Attacken auf die Computersicherheit meist einem Streben nach Gewinn zuzuordnen sind, gibt es daneben die großen Bot-Netze.

Diese werden dazu genutzt um entsprechende Attacken auf Server durchzuführen und bleiben vom Besitzer des einzelnen Rechners meist unbemerkt. Die Liste an Beispielen wäre hier nahezu unendlich. Bleibt festzuhalten, dass die deutsche Telekom im September 2014 konstatierte, dass im Schnitt täglich auf ihre Lockserver 450.000 versuchte Zugriffe erfolgen. Im Jahr 2012 kam es in den USA zu 12,6 Millionen Identitätsdiebstahlen (5% der erwachsenen Bevölkerung) mit einem Schadensvolumen von rund 9,8 Milliarden Dollar. Im selben Zeitraum wurden dort 10,8 Millionen Patientendaten missbraucht, um sich Zugang zu medizinischer Behandlung oder Medikamenten zu verschaffen.

Der staatliche Akteur

Während sich die Schadenereignisse der ersten beiden Kategorien von Tätern sich auf die unmittelbare Sachbeschädigung und Bereicherung beschränken, ist das von dieser Seite aus absichtlich herbeiführbare Schadenpotential nahezu unbegrenzt. Je technisierter eine Gesellschaft ist, desto grösser der denkbare Schaden. Alle Staaten mit nennenswerter technischer Infrastruktur bereiten sich auf die so genannte Hybride Kriegsführung vor. Kriegsführung ist insofern nicht ganz treffend, als die bewaffnete Auseinandersetzung eine irreversible und nicht abstreitbare letzte Eskalationsstufe in einem zwischenstaatlichen Konflikt darstellt. Allerdings würde Cyberkriegs-führung dann auch Verluste bei den Nichtkombattanten in einem Ausmaß ermöglichen, den herbeizuführen tausende täglich eingesetzter alliierter Kampfflugzeuge zwischen 1942 und 1945 nicht in der Lage waren.

Ein zweitägiger großflächiger Stromausfall führt gemäß einer Studie des BMI bereits zu merklichen sozialen Unruhen innerhalb der urbanen Bevölkerung. Wenn man dazu noch die absolute Abhängigkeit der "Just-in-Time"-Wirtschaft bei Logistik und Produktion in Deutschland dazu nimmt, wird ein solches Szenar wirklich angsterregend.

Da die privatisierte Telekom, aus nachvollziehbaren wirtschaftlichen Erwägungen, die komplette Umstellung des Telefonnetzes auf Voice Over Internet Protocol (VOIP) plant und damit die Abschaltung des analogen Kabelnetzes, wird sich ein solches Szenar in seiner Schadensauswirkung in spätestens fünf bis zehn Jahren potenzieren.

Die in der Folge aufgeführten Werkzeuge stammen aus einem Spiegel Artikel aus dem Jahr 2013 und sind in den abgelichteten Originalen auf das Jahr 2008 datiert. Somit sind sie als veraltet zu bewerten. Die Notwendigkeit, eine Raumüberwachung durch einen Einbruch zu installieren dürfte bei der rasant stattgefundenen technischen Entwicklung des *Internet-der-Dinge* in vielen Haushalten schon obsolet sein. In vielen Wohnstuben befinden sich nämlich mittlerweile:

- Playstation 4 mit Kamera und Internetzugang, bei der Nintendo Wii kommt noch ein Bewegungssensor hinzu.
- Internetfähiger Fernseher (neuerdings auch mit Mikro und Kamera!)
- Laptop mit Mikro, Kamera und Internetzugang
- Smartphone mit Mikro, Kamera, GPS Empfänger (inkl. Geräte-identifikation in den Telefonnetzen, beim Internetzugang und mittels Bluetooth)

Vor diesem Hintergrund ist ein Ansatz der persönliche Geräte im Dienstbetrieb zulässt, geradezu fahrlässig. Im Gegenteil, sollte sehr ernsthaft erwogen werden, dass Mitführen von Smartphones unter konsequenter Ahndung von Zuwiderhandlungen bei Sitzungen und Besprechungen zu verbieten!

Die Einkaufsliste für den staatlichen Akteur

Das Nachrichtenmagazin "Spiegel Online" veröffentlichte 2013 in seiner Rubrik Netzwelt eine interaktive Grafik (s. Link auf S. 19). Beim Inhalt handelt es sich laut Spiegel um einen internen Katalog der NSA, in dem Technikspezialisten Ausrüstung feilbieten - Preise inklusive.

Im Detail beschrieben werden dort Geräte für die Überwachung oder Manipulation von Servern, Firewalls, Routern / WLAN, Mobilfunk-geräten sowie Mobilfunknetzen beschrieben. Die aufgeführten Werkzeuge sind sicher nur ein Auszug aus dem Katalog, aus dem sich die zu den "Five Eyes"-Nationen angehörigen Nachrichtendienste bedienen können. Die Katalogdaten stammen aus 2008, das Angebot dürfte sich in den vergangenen Jahren sicher nicht verringert haben.

Bei den "Five Eyes" (USA, GBR, CAN, AUS und NZL) hatte man nun das Pech, mit Edward Snowden einen Whistleblower gehabt zu haben, der mal wieder mit einem USB-Stick voller Dokumente an die Öffentlichkeit ging.

Alle Dienste von Industriestaaten spielen da auf einem ähnlichen Niveau, also dürfte deren Werkzeugkasten ähnlich aufgebaut sein. Auf mindestens jedoch demselben Niveau spielen auch noch China, Indien und die russische Föderation. Hier sind entsprechende Anzeichen für die Vorbereitung *Hybrider Kriegsführung* spätestens seit der Eskalation der Krimkrise sichtbar. So gibt sich Russia Today als Sprachorgan der russischen Regierung zwar betont objektiv in der Berichterstattung, jedoch sieht das insbesondere seit der Eskalation auf die Ukraine bei dem Twitter-Ableger Sputnik schon ganz anders aus.

In der Ukraine werden neben der Propaganda durch Russland auch die Werkzeuge zur Instrumentalisierung von Minderheiten und daraus resultierend eine bewaffnete Auseinandersetzung durch diese Minder-heiten mit der Staatsmacht genutzt.

Dabei kann Moskau jederzeit beliebig den Konflikt aufheizen oder abkühlen lassen. Innerhalb dieser unübersichtlichen Gemengelage sind ähnliche Entwicklungen auch in Verbindung mit den baltischen Staaten und neuerdings beim Thema Spitzbergen (unter norwegischer Verwaltung) zu beobachten. Gleichzeitig taucht im europäischen Raum und den USA die Schadsoftware namens „Energetic Bear“ auf.

Ziel sind Unternehmen der Energiewirtschaft in den USA und Europa. In einem ersten Schritt nur zur Informationsgewinnung. Die identifizierte Schadsoftware ist allerdings auch in der Lage, durch entsprechende Steuerbefehle aktive Sabotage in den befallenen Systemen zu betreiben. Klarer Hinweis auf einen staatlichen Akteur und besorgniserregende Entwicklung ist, dass diese Schadsoftware bereits bei drei Herstellern von Mess- und Regeltechnik im Energie-versorgungsbereich innerhalb der standardmäßig ausgelieferten Steuersoftware nachzuweisen war. Damit kann auch bei einer vollkommenen physikalischen Trennung vom Internet ein Innentäter mit entsprechendem Zugang ein gewünschtes Schadensereignis auslösen. Dies wurde den Iranern mit Stuxnet schmerzhaft vor Augen geführt.

Dies ist natürlich argumentativ Wasser auf die Mühlen derer, die bereits vor der vorherrschenden Sachlage kapituliert haben. Absolute Sicherheit gibt es nicht! Dieses Totschlagargument hört man selten so häufig wie in Datenschutzdiskussionen.

Sachlich ist es mit Sicherheit zutreffend, allerdings lässt es sich auch auf alle anderen Lebensbereiche anwenden. Mit genau demselben Argument kann man Sicherheitsgurt, ABS, ASR und andere Sicherheitssysteme aus dem Auto verbannen. Es ist dann schön billig und trotz dieser Systeme sterben ja schließlich viele Menschen im Straßenverkehr. Wer sich dieser Sichtweise nicht vollumfänglich anschließen möchte, sollte beim Thema Datenschutz dann auch nicht den Kopf in den Sand stecken.

Abschließende Bewertung

Wie in allen Bereichen des Lebens ist auch beim Datenschutz immer eine Abwägung zwischen dem zu betreibenden Aufwand und dem damit erkauften Nutzen durchzuführen.

Die Täterkategorien eins und zwei sind durch Maßnahmen des Betriebes eines Netzwerkes unterschiedlicher Sicherheitsstufen relativ gut im Griff zu behalten. Daher ist es zwingend notwendig die Kernbereiche der Datenhaltung, in denen es insbesondere auf die Datenintegrität ankommt, redundant, räumlich verteilt, grundsätzlich verschlüsselt und ausfallsicher unter vollständiger eigener Kontrolle zu betreiben. Grundsätzlich wäre hier auch anzuregen, dass die Stadt sich durch das Lagezentrum des BSI unterstützen lässt und sich in die entsprechenden Notfallprozeduren einbinden lässt.

Bei Berücksichtigung dieser Aspekte dürfte ein großes Schadensereignis nahezu unwahrscheinlich sein. Die Angreifer der ersten beiden Kategorien haben die notwendigen Ressourcen für einen qualifizierten Angriff nicht. Selbst wenn sie darüber verfügen, steht der Aufwand in keiner Relation zum erwartbaren Nutzen und das Risiko gefasst zu werden ist aus ihrer Sicht unvertretbar hoch.

Für die dritte Täterkategorie erhöht sich der zu betreibende Aufwand, sich die für die in der zweiten Stufe benötigten Informationen zu beschaffen. Auch hier erhöht sich bei konsequenter Umsetzung der grundlegenden Maßnahmen die Wahrscheinlichkeit signifikant eine entsprechende Attacke vor dem Eintritt von Schadensereignissen zu erkennen und kontern zu können. Im zweiten Schritt der Infiltration von abgeschotteten Regel- und Steuernetzwerken muss der Angreifer dann einen entsprechend motivierten Innentäter suchen. Dies ist ohne den massiven Einsatz von nachrichtendienstlichen Mitteln und Methoden nahezu ausgeschlossen. Da auch staatliche Mittel begrenzt sind, ist bei einer entsprechenden Auslegung der kritischen Infrastrukturen auf kommunale Ebene das Risiko, Ziel einer solchen Aufmerksamkeit zu werden, als eher unwahrscheinlich einzustufen.

Der Aufwand potenziert sich in diesem Falle für den Angreifer, wenn man hier nicht auf große Netzwerke setzt, sondern auf dezentrale Netzwerke der einzelnen Anbieter.

Existentieller Baustein eines vernünftigen Datenschutzkonzeptes ist jedoch, dass Personal eingesetzt wird, welches den Anforderungen an die notwendige Vertrauenswürdigkeit gerecht wird. Daher ist Bestrebungen möglichst viel Personal auf dem freien Markt zu möglichst günstigen Preisen einzukaufen, energisch entgegen zu treten. Neben den Sicherheitserwägungen kann nur ein Personalkader im weiteren Betriebsablauf Optimierungen und sachbezogenen Ratschlag geben, der die Eigenheiten des Betriebsablaufes berücksichtigt und damit Fehlinvestitionen vorbeugt. Sofern bestimmte Dienstleistungen dann auf dem freien Markt zugekauft werden, sollte hier bestimmendes Kriterium sein, dass die bietenden Firmen sich vertraglich verpflichten nur Personal einzusetzen, welches gültige Sicherheitszertifikate der Sicherheits-behörden hat. Bei der Einhaltung dieser Kernforderungen sollte eine im Aufwand vertretbare und kosteneffektive Datensicherheit gewährleistet sein.

Links zu weiterführenden Informationen

Werkzeuge der NSA (Spiegel Online)
http://www.spiegel.de/netzwelt/netzpolitik/interaktive-grafik-hier-sitzen-die-spaeh-werkzeuge-der-nsa-a-941030.html

Berichterstattung zu dem Thema Energetic Bear
http://securityaffairs.co/wordpress/27224/cyber-crime/kaspersky-report-energetic-bear.html

http://www.symantec.com/connect/de/blogs/dragonfly-westliche-energieunternehmen-durch-sabotage-bedroht

Nationale Umsetzungsplanung zum Schutz Kritischer Infrastrukturen (UP-KRIITS)
http://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/upk_node.html

Bundesamt für Sicherheit in der Informationstechnik (BSI) Richtlinien
https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/technischerichtlinien_node.html

Personelle Sicherheit IT in Behörden
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Personalschaetzung/Arbeitshilfe_Personalschaetzung.pdf?__blob=publicationFile

Ergebnis der Prüfung IT und Stellungnahme Hauptamt 11/2014
https://www.duisburg.de/ratsinformationssystem/bi/vo0050.php?__kvonr=20065466&search=1

DS 15-0015 mit Anlage IT-Strategiekonzept
https://www.duisburg.de/ratsinformationssystem/bi/vo0050.php?__kvonr=20065608&search=1

Aktuelle kanadische Antiterror Gesetzgebung
https://en.wikipedia.org/wiki/Anti-terrorism_Act,_2015

Über den Autor

Kurt Klein, geboren 1967 in Krefeld, ist seit 1970 gemeldeter Bürger der Stadt Duisburg. 1989 folgten Abitur und die Prüfung zum staatlich geprüften elektrotechnischen Assistenten. Seit 1991 ist er als Beamter im Geschäftsbereich einer Bundesbehörde beschäftigt.

Seit Mitte der 90er Jahre ist der Autor mit dem Wachsen solcher Insellösungen auch auf Bundesebene vertraut. Seit 2000 ist er beauftragt mit der Konzeptionierung und Realisierung von Netzwerklösungen für Führungs- und Informationssysteme aller Behördenebenen, so wie der Datenbankentwicklung und -programmierung für Netzwerkanalysen.

Im Bereich der Sicherstellung der Datenschutzanforderungen in Nebenfunktionen war Kurt Klein bereits unter anderem tätig als IT-Beauftragter, Datenschutzbeauftragter, Verschlusssachenverwalter und Kryptobeauftragter in verschiedenen Dienststellen.

Insofern ist dem Autor also durchaus auch das Spannungsverhältnis zwischen Datenschutz und arbeitsfähigen Verwaltungsstrukturen bestens bekannt. Er ist der Meinung, dass beides in Einklang zu bringen ist, jedoch nicht zum Nulltarif und vor allem nicht durch ignorieren der real existierenden Bedrohungen für solche Systeme bei öffentlichen Verwaltungen.