ULD Sommerakademie 2014

25.08.2014, 08.30 - 17.00 Uhr,

ULD Kiel

Rede Andreas Könen, Vizepräsident des Bundesamtes für Sicherheit in der Informationstechnik

„Informationssicherheit in der digitalen Welt“

- es gilt das gesprochene Wort -

Begrüßung

Sehr geehrter Herr Dr. Weichert,
meine sehr geehrten Damen und Herren,

- ich bedanke mich sehr herzlich für Ihre Einladung und freue mich, vor Ihnen zum Thema „Informationssicherheit in der digitalen Welt“ vortragen zu dürfen.
- Die seit dem Sommer vergangenen Jahres allgegenwärtige Diskussion über die Enthüllungen des ehemaligen NSA-Mitarbeiters Edward Snowden verdeutlicht in besonderer Weise die Schlüsselstellung der Informationstechnik für Staat, Wirtschaft und Gesellschaft sowie die Chancen und Risiken der Digitalisierung.
- Gleichzeitig weist diese Debatte auf die Schnittmengen von Datenschutz und Informationssicherheit hin, die auch Thema einer eigenen BSI-Infobörse am heutigen Nachmittag sein werden.

Rahmenbedingungen/Entwicklungen: Technologie und Gefährdungslage

- Alles Handeln und Wirken – auch im Cybersicherheitsraum – hängt von Rahmenbedingungen bzw. Entwicklungen ab. Hierzu zählen insbesondere:
  1. die technologische Entwicklung sowie
  2. die Gefährdungslage.

1. Technologische Entwicklung: IT-Durchdringung und -Vernetzung führt zur Digitalisierung

- Über Cyber-Sicherheit in diesen Tagen zu reden, bedeutet natürlich, die weiterhin kritische Gefährdungslage zu berücksichtigen. Bevor ich hierauf eingehe, lassen Sie mich bitte auf ein grundsätzliches Sicherheitsdefizit bei der Festlegung der Internetstandards hinweisen, das den Cyberraum bis heute beeinträchtigt:
- Das Internet wurde Ende der 1960er Jahre unter dem Aspekt hoher Verfügbarkeit als Projekt des US-Verteidigungsministeriums gefördert und hat sich von einem Computerverbund von Universitäten und Forschungseinrichtungen ab den neunziger Jahren rasch zu einem weltumspannenden Netz entwickelt.
- Durch den weitgehenden Verzicht auf Kryptografie können die Vertraulichkeit und Integrität durch die ursprünglich definierten Internetstandards nicht hinreichend gewährleistet werden (z.B. sind Mails offen wie Postkarten), wodurch die Möglichkeiten für IT-Ausspähungen und Cyberangriffe gefördert werden.
- Die Ursprünge des Internets waren in einem Einsatzszenario eingebettet, in dem IT-Security by Design, also der frühzeitige Einbau von vertraulichkeitsfördernden Sicherheitsmechanismen, nicht vorgesehen war.
- Die Einsatzszenarien von IT in der digitalen Welt des 21. Jahrhunderts waren sicherlich vor 30 oder 40 Jahren nicht absehbar. Heute aber stellen uns Schwachpunkte in Technologien oder der Konstruktion des Internets vor dem Hintergrund der immer weiter voranschreitende Digitalisierung unserer Gesellschaft vor erhebliche IT-Sicherheitsprobleme und liefern auch den methodischen Ansatzpunkt vieler Cyberangriffe.
- Diese „Konstruktionsfehler“ sowie ein fehlendes IT-Sicherheitsbewusstsein setzen sich bis heute in den neuesten Technologien oder Diensten wie etwa Cloud Computing oder Smartphones fort - denn vielfach geht Funktionalität der Sicherheit voraus. Dies gilt besonders für Bereiche, in denen durch neue Funktionalitäten Kunden geworben werden sollen, deren Sicherheitsbewusstsein noch nicht stark ausgeprägt ist.
- An dieser Stelle sei auch auf die aus betriebswirtschaftlichen Notwendigkeiten heraus resultierende Tendenz in Unternehmen hingewiesen, die IT-gesteuerten Produktionsprozesse mit der Unternehmens-IT zu vernetzen und damit die Produktionsstraßen mit dem Internet zu verbinden, ohne dies durch hinreichende Sicherheitsmaßnahmen zu

flankieren.

2. Gefährdungslage: Lage ist weiterhin kritisch

- Diese grundsätzlichen Netzprobleme sind nur eine Erklärung, warum die heutige Gefährdungslage weiterhin kritisch ist.
- Neben einer Vielzahl potenzieller Angriffsziele (alles mit einer Verbindung zum Internet ist attackierbar) bietet das Internet einen hohen Grad an Anonymität (geringes Entdeckungsrisiko) sowie die Aussicht auf große finanzielle Gewinne bzw. Informationsgewinne.
- So zeigen die neuesten Zahlen des Cyber-Sicherheitslagebilds des BSI, dass:
  - pro Monat mit 6,5 bis 7,1 Millionen Schadprogrammen - teilweise nur Varianten bereits bekannter Schadprogramme - gerechnet werden muss,
  - von mehr als einer Millionen infizierten Webseiten auszugehen ist (etwa 3 %),
  - Identitätsdiebstahl hoch im Kurs liegt: Im Januar und April 2014 warnte das BSI vor millionenfachem Identitätsdiebstahl,
  - der Regierungsinformationsverbund ein Ziel ist: täglich gibt es 2.000 bis 3.000 Angriffe normaler Qualität.

Fazit: Es sind alle Zielgruppen betroffen: Staat, Wirtschaft und Bürger.

<u>Kommerzielle Flächenangriffe</u>

- Die Masse der Angriffe, insbesondere auf Bürger, hat einen kriminellen Hintergrund. Vor allem dann, wenn es um Identitätsdiebstahl, Cybererpressung und Spamverteilung geht.
- Man muss nicht zwingend Falltüren in IT-Produkte einbauen, um in IT-Systeme eindringen zu können.
- Bereits mit bekannten, noch nicht gepatchten Schwachstellen (und erst recht mit Zero-day-Exploits, d.h. Schwachstellen, die bislang unbekannt sind) kann wirksam in IT-Systeme eingedrungen werden, wenn ein Administrator eine Sicherheitslücke nicht rechtzeitig schließt oder schließen kann.
- Im Internet werden z.B. Angriffsmöglichkeiten über Botnetze für geringe Beträge ange-

boten. Für hochwertigere Schadprogramme gegen bisher nicht entdeckte Schwachstellen werden Beträge in bis zu fünfstelliger Höhe gezahlt.

- Die Internetkriminalität hat sich gut aufgestellt und muss, wenn man sich die einschlägigen Webseiten ansieht, auch sehr gut verdienen. Über Botnetz-Angriffe können leicht Millionenbeträge erzielt werden.
- Die positive Nachricht ist, dass sich etwa 80 - 90 % der Bedrohungen der Kategorie von Cyberangriffen zuordnen lassen, die hinsichtlich ihrer Qualität mit bekannten Standardsicherheitsmaßnahmen abgewehrt werden können.
- Grundsätzlich gilt: Präventive Maßnahmen sind ein wesentlicher Baustein, um angemessen auf die kritische Gefährdungslage zu reagieren. Besonders gefährdete Bereiche müssen jedoch auch Bedrohungen Rechnung tragen, die von hochprofessionellen Cyberkriminellen oder Nachrichtendiensten ausgehen.

<u>NSA-Affäre</u>

- Die Verletzbarkeit der IT und der IT-Infrastrukturen wurde uns besonders plastisch durch die Snowden-Enthüllungen vor Augen geführt, deren Veröffentlichung vor fast genau einem Jahr, Anfang Juni 2013, einsetzte.
- Dass staatliche Stellen die Kommunikation im Internet und in anderen öffentlichen Netzen überwachen, ist nicht neu. Selbst Fachleute waren jedoch über das enorme Ausmaß und die Dichte der Überwachungsmaßnahmen überrascht, die in den Snowden-Dokumenten dargestellt werden. Insbesondere war auch der erhebliche Ressourcenaufwand in diesem Umfang nicht erwartet worden.
- Aber auch ganz unabhängig von staatlichen Aktivitäten zeigen die Enthüllungen, was mit entsprechenden Fähigkeiten und Ressourcen leistbar ist und was für Ausspähmöglichkeiten existieren, die jeden - staatliche Institutionen, Wirtschaft, Wissenschaft und Bürger - treffen können.
- Eine Beschreibung der Gefährdungslage und geeignete Sicherheitsmaßnahmen müssen in einer Gesamtbetrachtung deshalb neben nachrichtendienstlichen Gefährdungen auch Cyberangriffspotenziale anderer Staaten und Organisationen berücksichtigen.
- Angesichts dessen stellt sich die Herausforderung, wie der Schutz der Privatsphäre

und der Vertraulichkeit im Internet gewährleistet werden kann. Die Frage der Vertrauenswürdigkeit überträgt sich auch auf die IT-Marktführer,. Die Enthüllungen suggerieren eine partielle Zusammenarbeit einiger Firmen mit der NSA.

- Aus einer technischen Perspektive kann festgehalten werden, dass die Enthüllungen nachrichtendienstliche Angriffswege und Gefährdungen auf drei Ebenen aufzeigen:
  - Strategische Aufklärung in Netzen durch weltweiten Zugriff auf Internetknoten, -kommunikation und -dienste,
  - Individualisierte Lausch- und Cyberangriffe gegen ausgewählte Netzwerke, Institutionen und Personen sowie
  - Manipulation wichtiger IKT-Komponenten und -Systeme.

- Die Gefährdungsszenarien im Bereich der mobilen Kommunikation verdeutlichen diese unterschiedlichen Ebenen exemplarisch, da in diesem Bereich fünf Angriffswege wesentlich sind, die mit den drei Ebenen korrelieren.
- So kann im Bereich der mobilen Kommunikation ein unbefugter Zugriff auf Kommunikationsdaten durch
  - Manipulation des Endgerätes (<> Manipulation von IKT-Komponenten),
  - Abhören von Endgeräten in räumlicher Nähe (<> Individualis. Lauschangriffe),
  - Abhören von Funkwellen aus der Ferne (<> Individualis. Lauschangriffe),
  - Überwachungstechnik im Netz (<> Manipulation von IKT-Komponenten und / oder strategische Aufklärung in Netzen) oder
  - Überwachungsmaßnahmen in ausländischen Netzen (<> Strategische Aufklärung in Netzen)

  erfolgen.
- Mobile Kommunikation ist somit potenziell durch Überwachungsmaßnahmen auf al-

len drei Angriffsebenen gefährdet, sodass auch die Schutzmaßnahmen, auf die ich im Nachfolgenden zu sprechen komme, unterschiedliche Angriffsebenen adressieren müssen.

Zielsetzungen und Maßnahmen zur Verbesserung der Risikosituation im Cyberraum

- Die zentralen Ziele aus technischer Sicht müssen sein:

  - Die Risiken der Digitalisierung - also der technologischen Entwicklung - adäquat zu adressieren.

  - Zielgruppengerechte Maßnahmen zu ergreifen bzw. die Wirtschaft und besonders die Bürgerinnen und Bürger beim Selbstschutz zu unterstützen.

Hierzu möchte ich Ihnen im Folgenden vier Maßnahmenbereiche konkret vorstellen:

1. Vertrauenswürdige Krypto- und Cybertechnologien durchgängig zur Anwendung bringen

1.1. Kryptotechnologien

- Starke Kryptoalgorithmen, Zufallszahlengeneratoren und Protokolle einsetzen.
- Implementierung durch kompetente und vertrauenswürdige Hersteller fördern und beauftragen.
- Flexible und leicht nutzbare Public Key-Infrastrukturen entwickeln, speziell für Browser, und auf Basis sicherer eID-Lösungen wie beispielsweise dem neuen Personalausweis (nPA).

1.2. Cybertechnologien

- Durchgängige Strukturierung von Netztopologien unter Sicherheitsgesichtspunkten (sowohl Internet- als auch Firmennetze!).
- Firewalls, Virenscanner und Schadprogramm-Erkennungssysteme weiterentwickeln und einsetzen.
- Fragmentierte Cybersicherheitslagebilder gemeinsam mit allen Playern in der Wirtschaft, speziell KRITIS und Allianz für Cybersicherheit, zu einem Gesamtlagebild Deutschland fortentwickeln.

Das BSI stellt Krypto- und Cyberprodukte bereits für die öffentliche Verwaltung sowie im EU- und NATO-Kontext zur Verfügung → Jedoch besteht Forschungs- und Entwicklungsbedarf, um Lösungen auch für weitere Zielgruppen zu entwickeln!

2. „Digitale Autonomie“ fördern

Was bedeutet dieser Maßnahmenbereich konkret? Teilaspekte sind z.B. die

- Informationelle Selbstbestimmung (umfasst aber nicht nur Datenschutz),
- Awareness über die eigene (Cyber-)Sicherheitslage,
- Transparenz bei der Nutzung von Netzen und Cloud-Diensten (Wo sind meine Daten? Wer hat potenziell Zugriff darauf?)

oder die Auseinandersetzung mit Fragen wie beispielsweise

- Sind die verwendeten Produkte und Dienstleistungen vertrauenswürdig?
- Gibt es Alternativen zu den bis dato genutzten Technologien?

Hierzu ist es Aufgabe des BSI, insbesondere mit Blick auf die Zielgruppe der Bürger,

- Bildungsangebote im Bereich der Cybersicherheit zu initiieren,
- die Cybersicherheitslage zu kommunizieren und
- die Vertrauenswürdigkeit von Angeboten transparent zu machen.

Letztgenannter Aspekt führt zu Punkt 3.:

3. Die Qualität von Informationssicherheitsprodukten und -dienstleistungen sicherstellen

durch die Instrumente

- Standardisierung und Zertifizierung (IT-SiGe)

dabei sind Maßnahmen geboten wie etwa

- das Zusammenwirken mit Herstellern aus Deutschland in Leuchtturmprojekten,
- die verstärkte Berücksichtigung von Sicherheitsanforderungen bei öffentlichen Beschaffungen oder
- die Förderung der IT-Sicherheitsforschung.

4. Notfall- und Krisenfertigkeit + „Resilienz“

Bei Cybersicherheits-Vorfällen ist es wesentlich,

- klare Notfallpläne bereitzuhalten,
- in einer eingeübten Art und Weise Cybersicherheitsmaßnahmen in der IT durchzuführen, etwa
  - Angreifer-Aktionen zu identifizieren,
  - zu warnen,
  - Netze abzuschalten,
  - Alternative IT zum Einsatz zu bringen,
  - Unterstützung von außen einzufordern und anzunehmen.

Jedoch gibt es Engpässe:

- nationales Angebot in der Wirtschaft zu klein,
- Forensiker und Incident Response Teams werden dringender denn je benötigt.

Schlussbemerkung/Rollenverständnis und Positionierung des BSI

- Grundsätzlich gilt: Das Vertrauen der Anwender erwerben wir nur durch Transparenz und Zuverlässigkeit bei den eingesetzten IT-Sicherheitssystemen. Hierfür brauchen wir aber auch Vertrauen in die Akteure - seien es staatliche Stellen, Hersteller oder Dienstleister. Das BSI sieht sich in seinem gesetzlichen Auftrag „der Förderung der IT-Sicherheit in Deutschland“ auch als ein Vertrauensanker und als neutrale Stelle im Wettbewerb.
- Neben der Schutzfunktion für die Regierungsnetze hat das BSI eine Warn- und Standardsetzungsfunktion im Interesse der Bürger und Wirtschaft (→ durch Mindeststandards oder technische Richtlinien). Die Wahrnehmung erfordert eine breite fachliche Aufstellung in der IT-Sicherheit mit schwerpunktmäßig tiefer fachlicher Expertise. In der Kooperation mit der Wissenschaft wird diese Kompetenz in der Breite und Tiefe weiterentwickelt.
- In diesem Sinne verstehe ich auch die Aussagen aus der Politik zu einem Ausbau der Rolle und Verantwortung des BSI in den nächsten Jahren.
- Ich bedanke mich für Ihre Aufmerksamkeit!