Dr. Harald Müller-Witt; Zero Emissions, Inc.

Initiative für ein CyberSpace-Institut NRW

Prof. Dr. Paolo E. Verissimo lehrt an der TU Lissabon (Departamento de Informática) und ist einer der weltweit führenden Experten im Bereich Information Infrastructure Security and Dependability[1]. Bereits 2003 konnte er auf Sicherheitskonferenzen die Verwundbarkeit von SPX Steuersystemen (Industriestandard) nachweisen, deren Parameter sich durch einfaches Überschreiben ändern ließen. Eine Sicherheitslücke, die in der Folge der (wahrscheinlich Amerikanisch-Israelische) Wurm STUXNET 2010 ausnutzte, um das Iranische Atomprogramm zu sabotieren. Dieser Cyber-Angriff zerstörte mind. 20% der iranischen Gaszentrifugen, schlicht durch die lange Zeit unbemerkt gebliebene Modulation der max. und min. Drehzahlen[2].
Prof. Verissimo übernimmt ab September 2014 für die kommenden drei Jahre den mit 5 Mio. € aus der Luxemburgischen Exzellenzinitiative (PEARL) geförderten Aufbau und die Leitung des neugeschaffenen „Interdisciplinary Center for Security, Relyability and Trust" (SnT) an der Universität Luxemburg[3].

Der Grund, warum das knapp 550.000 Einwohner große Luxemburg, relativ betrachtet, derartig hohe Geldbeträge einsetzt, erscheint uns – mit Blick auf NRW, das analog 159 Mio. € investieren müsste – bemerkenswert.

Seit dem Bekanntwerden der NSA Cyberspionage Affäre versuchen die Sozialen Netzwerke aus den USA (Google, Facebook, Twitter, Yahoo u.a.) verlorenes Vertrauen ihrer Kund_innen dadurch zurück zu gewinnen, dass sie einen Teil ihrer Aktivitäten und ihrer Server Landschaften aus den USA auslagern, um nicht mehr per US-Gesetzgebung gezwungen werden zu können, private Informationen massenhaft zur Verfügung zu stellen.

So wie Irland mit seiner 12%igen Körperschaftssteuer ein attraktiver Standort für die IT-Hardware-Industrie wurde, strebt Luxemburg Gleiches auf dem Gebiet der Sozialen Netzwerke an. Nur Steuervorteile allein reichen diesmal nicht: Was die Internet Giganten vielmehr als Gegenleistung für die Verlagerung ihrer Europäischen Head Quarter nach Luxemburg forderten, war ein sicherer Hafen für ihre Datenbestände und eine stabile, maximal mögliche IKT-Sicherheitsstruktur.

Spätestens an diesem Punkt sollten wir uns fragen:

- Wenn Cyber-Crime und Cyber-War ganze Länder bzw. deren Industrien bedrohen können und andererseits
- verlässlich geschützte Infrastruktur und ITK-Systeme, sowie eine vorausschauende und abwehrbereite Forschungslandschaft ein immer deutlicherer Standortvorteil im internationalen Ansiedlungswettbewerb werden

wo stehen wir diesbezüglich in NRW? Was haben, was hätten wir zu bieten?

---

[1] Lebenslauf Prof. Dr. Paolo E. Verissimo. In: http://www.di.fc.ul.pt/~pjv (letzter Zugriff: 22.06.2015).

[2] Wikipedia (2015): Stuxnet. In: https://en.wikipedia.org/wiki/Stuxnet (letzter Zugriff: 22.06.2015).

[3] Interdisciplinary Centre for Security, Reliability and Trust. In: http://wwwen.uni.lu/snt (letzter Zugriff: 22.06.2015).

Ein Blick auf die Industrielandschaft in NRW zeigt, dass allein in sechs der neun als besonders kritisch eingestuften Infrastruktursektoren (gem. KRITIS Definition) eine Reihe nationaler Schwergewichte beheimatet sind. So finden wir z.B. im Bereich

- **Energie:** drei der größten Energieversorger (E.ON, D; RWE, E; STEAG, E) sowie zahlreiche große und mittelgroße Stadtwerke
- **Verteilernetze**: Strom: Amprion, DO; TenneT; Arnheim, NL (ganz Ost- NRW)
  Gas: Ruhrgas, E sowie zahlreiche große und mittelgroße Stadtwerke
  Wasser: Gelsenwasser, GE (Stadtwerke DO & BO) und abermals zahlreiche große und mittelgroße Stadtwerke
- **ITK:** Telekom[4], BN; Vodafone, D; E-Plus, D
- **Transport und Logistik:** Duisport; DU
- **Ernährung:** Metro, D
- **Finanz- und Versicherungswesen:** allein neun der zwanzig größten Versicherungskonzerne haben ihren Sitz in NRW, darunter ERGO, D; AMB Generali, K; AXA, K und Gothaer, K

Ein Blick auf die Hochschullandschaft zeigt, dass in NRW zwar 80 Masterstudiengänge der Fachrichtung Informatik angeboten werden, doch darunter ist nicht einer mit dem Schwerpunkt Sicherheitsinformatik. Zersplittert und über das Land verteilt gibt es verschiedene Lehrstühle, die sich mit der Problematik beschäftigen, doch IT-Sicherheit ist kaum Pflichtfach. Mit dem Fraunhofer Institut für Umwelt, Sicherheits- und Energietechnik (UMSICHT) in Oberhausen ist sogar eine Großforschungseinrichtung in NRW thematisch damit befasst und im Herbst 2012 vereinbarte die FH Aachen erstmals eine Kooperation die vorsieht, dass Studierende bei den Expert_innen für Computerforensik im Cybercrime-Kompetenzzentrum des LKA NRW hospitieren und umgekehrt LKA Mitarbeiter_innen Seminare an der FH besuchen.

So löblich und notwendig das auch ist, reicht es aus, um NRW im Wettbewerb zu positionieren und seine kritische Infrastruktur zu schützen? Nutzen wir die Talente und das Potenzial unserer Hochschulen in einer zielgerichteten und der Bedrohungslage angemessenen Weise?

Wozu motivierte Student_innen in der Lage sind, demonstrierte im Juli 2014 ein Team der Zhejiang University. Es gewann auf der Security for Asia Network (SyScan360) den ausgelobten $10,000 Preis für den erfolgreichen Hack eines Tesla Model S. Das Kapern der vitalen Systeme des Fahrzeugs gelang dabei erstmalig während der Fahrt und über mobile Schnittstellen. Der Hersteller des e-Sportwagens war dankbar und erklärte: "we support the idea of providing an environment in which responsible security researchers can help identify potential vulnerabilities."[5]

Auf Seiten der Behörden wurde, unter Federführung des Bundesinnenministeriums ab 2003 mit dem systematischen Aufbau einer Cybersicherheitsstrategie begonnen. Ziel ist es, die Abwehrmaßnahmen der Akteure aus Bund, Länder, Wirtschaft und Öffentlichkeit zu vereinheitlichen. In 2005 verabschiedete das Kabinett den „Nationalen Plan zum Schutz der

[4] Telekom (2015): Übersicht über die aktuellen Cyberangriffe (aufgezeichnet von 180 Sensoren). In: http://www.sicherheitstacho.eu/ (letzter Zugriff: 22.06.2015).

[5] Korzeniewski, Jeremy (2015): Testa Modell S succesfully hacked by Zhejiang University team. In: http://www.autoblog.com/2014/07/18/tesla-model-s-successfully-hacked-by-zhejiang-university-team/ (letzter Zugriff: 22.06.2015).

Informationsinfrastrukturen in Deutschland".[6] 2009 beschloss die Bundesregierung darauf aufbauend die „Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS)".[7] Im Rahmen von KRITIS kooperieren nicht nur verschiedene Bundesbehörden (BMI, BSI, BKA, BBK) und diverse Landesämter (u.a. LKA-NRW), vielmehr ist es erklärtes Ziel, durch regelmäßigen Austausch mit den Betreibern kritischer Infrastrukturnetze und deren Verbänden konkrete Maßnahmen und/oder Umsetzungsempfehlungen zu entwickeln und zu implementieren. Dadurch angeregt haben sich etwa dreißig große Infrastrukturunternehmen mit einem hohen Grad an IT-Abhängigkeit freiwillig zur Einhaltung eines gemeinsamen Mindestniveaus an IT-Sicherheit verpflichtet. Zusätzlich zu den fest installierten Arbeitsgruppen lädt das BSI einmal im Jahr zu einer großen Wirtschaftskonferenz, die dem Erfahrungsaustausch und der Sensibilisierung der Teilnehmer_innen hinsichtlich der neuesten Bedrohungspotenziale dient.

Richtungsweisend in diesem Zusammenhang ist auch die enge Kooperation des LKA-NRW und (seit 2013) des LKA-BaWü mit dem IT-Branchenverband BITCOM, von dem beide Seiten profitieren. Die Polizeibehörden wissen in der Regel früher, mit welchen neuen Methoden bzw. Techniken die Cyber-Kriminellen arbeiten, was der Industrie bei vorbeugenden Maßnahmen hilft. Umgekehrt können die LKA-Cyber-Kompetenzzentren rasch auf Programmierer_innen oder Netzspezialisten_innen der Industrieseite zurückgreifen, wenn es um ad-hoc Gefahrenabwehr oder Prävention geht.

Bei der Entwicklung von „Methoden zur Reduzierung des Ausfallrisikos der Stromversorgung" im Rahmen von GRASB[8], einem Teilprojekt zum Schutz der kritischen Infrastruktur (KRITIS), wirken neben dem TÜV-Nord und der FH-Köln aus NRW auch die E.ON AG, die RheinEnergie AG und die SW-Duisburg AG mit. Um zu praxisrelevanten Aussagen zu kommen, wird dabei das Stromversorgungssystem über die gesamte Wertschöpfungskette erfasst und kritische Prozesse werden ermittelt. Ob diese kritischen Prozesse anschließend einem simulierten Angriff ausgesetzt wurden, geht aus den bisher veröffentlichten Dokumenten nicht hervor.

Als vorläufig vorletzten Schritt im Rahmen ihrer Abwehrmaßnahmen, hob die Bundesregierung in 2011 das Nationale Zentrum für Cyber-Abwehr (NZCA) aus der Taufe und erweiterte gleichzeitig den Kreis der beteiligten Behörden um das Bundesamt für Verfassungsschutz (BfV). Die Cyber-Sicherheitsstrategie verantwortet seither der „Cyber-Sicherheitsrat", dem die Beauftragte der Bundesregierung für Informationstechnik vorsteht.

Es geht nicht darum, die Bemühungen der vergangenen Jahre von Seiten der Behörden und der Industrie schmälern zu wollen, aber die jüngst durch Edward Snowden öffentlich gemachten, allumfassenden, gesetzeswidrigen Lauschangriffe von GCQQ (UK) und NSA (USA) auf die Kommunikation von und zwischen Bürger_innen, Regierungen und Unternehmen, offenbarten die erschreckende Unfähigkeit unserer nationalen Behörden, bzw. der durch sie koordinierten

[6] Bundesministerium des Inneren (Hrsg.) (2008): Der „Nationale Plan zum Schutz der Informationsinfrastrukturen in Deutschland" als umfassende Dachstrategie zu IT-Sicherheit. In: http://www.bmi.bund.de/SharedDocs/Standardartikel/DE/Themen/OeffentDienstVerwaltung/Informationsgesellschaft/NPSI.html (letzter Zugriff: 22.06.15).

[7] Bundesministerium des Inneren (Hrsg.) (2009): Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). In: http://www.bmi.bund.de/cae/servlet/contentblob/544770/publicationFile/27031/kritis.pdf (letzer Zugriff: 22.06.2015).

[8] Bundesamt für Bevölkerungsschutz und Katrastrophenhilfe (Hrsg.) (2005): Projekt GRASB. In: http://www.bbk.bund.de/DE/AufgabenundAusstattung/KritischeInfrastrukturen/Projekte/GRASB/GRASB_Startseite.html?nn=1899916 (letzter Zugriff: 22.06.2015).

Cyber-Abwehraktivitäten, zeitnah und lückenlos Bedrohungen dieser Art aufzudecken, geschweige denn zu verhindern.

Wer tiefer bohrt und hinter die Kulissen blickt, dem wird schnell klar, dass es die zehn Mitarbeiter[9] im deutschen NZCA unmöglich mit den 100.000 Beschäftigten der NSA aufnehmen können. Selbst die 600 Beschäftigten[10] im BSI, die auf 730 aufgestockt werden sollen, verschieben das Kräfteverhältnis nur marginal und auch die 29 Mio. €[11], mit denen die Regierung ihre Digitale Agenda unterfüttert. Vollends hilflos wirkt das zuständige Innenministerium, wenn es ausgerechnet von der US-Armee verlegte Leitungsrohre für die (Hochsicherheit) „Netze des Bundes" (NdB) ankaufen und die Installationsarbeiten z.T. von US-Tochterfirmen durchführen lassen will, die im Zuge der Snowden Enthüllungen wiederholt als Spionagehelfer enttarnt wurden[12].

Seit Snowdens Enthüllungen kann zudem als gesichert gelten, dass das Auftragsprofil der NSA explizit auch Industriespionage umfasst. Neben den USA droht besondere Gefahr aus Russland und China. Eine Untersuchung des US- Sicherheitsspezialisten Symantec ergab, dass 2012 ein Viertel aller Versuche, Firmen auszuspionieren, von China ausging[13]. Westliche Geheimdienste bringen solche Hackerattacken seit Jahren mit der Volksbefreiungsarmee in Zusammenhang, die in ihrer Fremdsprachenschule in Luoyang und an der University of International Relations in Nanjing gezielt Spezialist_innen ausbilden lässt. So könnte es sich rächen, dass die liberale Sicherheitsarchitektur der Bundesregierung bisher überwiegend auf Koordination setzt und den Selbstschutz der Unternehmen und Privathaushalte propagiert[14].

Wie kann also, wie muss die Industrie hierauf reagieren? Klar ist, dass der Kauf von Virenprogrammen und Firewalls, mit dem zahlreiche klein- und mittelständische Unternehmen glauben sich schützen zu können, längst nicht ausreicht. Auf Produktseite ist die Sicherheitszertifizierung einzelner Komponenten, Produkte, Produktgruppen oder ganzer Entwicklungsstandorte nach dem BSI-Standard ein probates Gegenmittel. Auf der Systemseite, im Zusammenspiel von Organisation und Mitarbeiter_innen, bedient man sich hilfsweise einer Zertifizierung nach dem ISO/IEC 27001 Standard. Damit weist das Unternehmensmanagement intern wie extern nach, dass ein IT-Sicherheitsmanagement vorhanden ist und zumindest während der Auditierung ein definiertes IT-Sicherheitsniveau erreicht wurde. Die erfolgreiche Abarbeitung von Audit-Checklisten ist somit eine notwendige, doch keinesfalls hinreichende Vorbedingung, um dauerhaft geschützt zu sein.

Was eigentlich erforderlich wäre, nämlich das eigene Firmennetz unregelmäßig durch „weiße" Hacker attackieren zu lassen, um Schwachstellen und Sicherheitslücken schneller aufzuspüren, lebt Daimler-Benz als einer der wenigen deutschen Konzerne mit einer eignen Hacker-Spezialeinheit vor.[15] Selbst wenn sich damit nicht jedes Fremdeindringen hundertprozentig

[9] Süddeutsche Zeitung : „Zeit für Visionen". (2014) Nr. 187.

[10] ebenda

[11] Wirtschaftswoche: „Firmen rüsten auf". (2014) Nr. 35.

[12] Baumgärtner, Maik/ Knaup, Horand/ Müller, Peter/ Schindler, Jörg: Die Röhre der anderen. In: Spiegel (2014) Nr. 44.

[13] Krone (2011): China bestätigt heimlichen Aufbau von Cyberarmee. In: http://www.krone.at/Digital/China_bestaetigt_heimlichen_Aufbau_von_Cyberarmee-Albtraum_fuer_Westen-Story-265520 (letzter Zugriff: 22.06.2015).

[14] Berke, Jürgen: IT-Sicherheit wie im wilden Westen. In: Wirtschaftswoche (2014) Nr.34.

[15] Berke, Jürgen: Geheime Mission. In: Wirtschaftswoche (2014) Nr. 31. S.42

ausschließen lässt, so bleibt dennoch im Ergebnis richtig, die Widerstandsfähigkeit der IT-Systeme massiv hochzuschrauben, dass es für potenzielle Angreifer sehr (zeit)aufwendig wird und insoweit ihr Risiko steigt, rechtzeitig entdeckt zu werden.

Die nächste Sicherheitslinie und logische Ergänzung wäre, ausgehend vom Endproduzenten und der Wertschöpfungskette folgend, die Zulieferer und, sofern kritisch, auch die Großabnehmer in die White-Hack-Systematik mit einzuschließen.

Und, gerade was die Firmen aus dem Bereich kritische Infrastruktur (KRITIS) anbelangt, wird man nicht umhin kommen, für den Datenaustausch zwischen diesen Teilnehmer_innen sowie ihren vor- und nachgelagerten Geschäftspartner_innen

- verbindliche Sicherheitsvorschriften zu erlassen und deren Einhaltung zu kontrollieren
- ein besonders gesichertes Netz zu nutzen (wie z.B. das ENX in der Automobilindustrie)
- eine gemeinsame Verschlüsselungssoftware zu vereinbaren und darüber zu kommunizieren
- jeden erkannten Cyberangriff meldepflichtig zu machen[16] und
- diese in einem öffentlich einsehbaren Register zu dokumentieren[17].

Unsere Auffassung, dass insbesondere im Bereich der kritischen Infrastruktur das bislang auf Behördenseite dominierende Fordern und Fördern durch rechtsverbindliche Festlegungen und systematische, strafbewehrte Kontrollen zu ergänzen ist (incl. Einbeziehung der Altsysteme[18]), findet nicht nur in der IT-Sicherheitsindustrie Anklang, die daran verdient. Auch Verwaltungsjuriste_innen sehen mit Sorge, dass derzeit keine gesetzliche Verpflichtung zu Umsetzung des IT-Sicherheitskatalogs der Bundesnetzagentur besteht[19]. Ob und inwieweit hier der letzte, gerade beschlossene Sicherheitskatalog der Bundesregierung, die „Digitale Agenda", zu einem Umsteuern bis hinab in die Verästelungen der Umsetzungsverordnungen und des Verwaltungshandelns führen wird, muss sich erst noch weisen.

Ausgehend von unserer Fragestellung: Wo stehen wir bezüglich der Netzsicherheit in NRW, was haben, was hätten wir zu bieten, müssen wir nach Lage der Dinge feststellen, dass die, unter der Zuständigkeit des Bundes und Mitwirkung der Länder bislang eingezogenen IT-Sicherheitsstrukturen schon heute nicht ausreichen, um die vorhandene Netzinfrastruktur und die auf sie angewiesenen kritischen Sektoren zu sichern. Wie bei einem Has` und Igel Rennen drohen wir stattdessen noch weiter ins Hintertreffen zu geraten, denn die technologische Entwicklung schreitet mit riesen Sprüngen voran. Hier ein Vorgeschmack auf das, was uns erwartet.

Im produzierenden Gewerbe arbeiten Forschungseinrichtungen und Betriebe mit Hochdruck an der Verbindung von realer und virtueller Fertigungswelt (Stichwort: Industrie 4.0). Angestrebt wird dabei nicht weniger, als die nahtlose Integration von Informations-, Kommunikations- und Automatisierungstechnologien über sämtliche Betriebsabläufe und die gesamte

[16] Bundesministerium für Wirtschaft und Energie/ Bundesministerium des Inneren/ Bundesministerium für Verkehr und digitale Infrastruktur (Hrsg.) (2014): Digitale Agenda 2014-2017. S. 32.

[17] Vollkorn (2014): Stand der Technik nicht genug: CC fördert Risikobewertung für Sicherheit im Stromnetz. In: http://www.ccc.de/de/updates/2014/BNetzA (letzter Zugriff: 22.06.2015).

[18] ebenda

[19] Lied, Andreas et. Al.: Der IT-Sicherheitskatalog der Bundesnetzagentur: Auswirkungen auf die Verteilnetzbetreiber. In: Energiewirtschaftliche Tagesfragen (2014) Nr. 8. S. 67.

Wertschöpfungskette hinweg. In der Umsetzung läuft das darauf hinaus, dass an den Schnittstellen der beteiligten Unternehmen einige wenige standardisierte SW-Protokolle und Hardwarekomponenten für den reibungslosen Austausch und die Weiterverarbeitung in der Kette sorgen. Da alles mit allem zusammenhängt steigt die Verwundbarkeit, denn jede unbeabsichtigte oder gar absichtlich herbeigeführte Störung (STUXNET als Blaupause) kann sich kaskadenförmig durch das System fortpflanzen oder, schlimmer noch, aufschaukeln.

Im Anlagen- und Maschinenbau geht der Trend immer mehr in Richtung vorbeugende Wartung. Durch den Einbau von zahllosen Sensoren, die die Vibrationen, Geräusche, Drücke, Verbräuche und Umgebungsparameter der ausgelieferten Maschinen und Anlagen kontinuierlich messen und aufzeichnen, gelingt es, mithilfe intelligenter Datenfernauslesung und –auswertung, aufkommende Probleme so rechtzeitig zu identifizieren, dass ein Maschinenschaden mit zwangsweisem Produktionsstillstand erst gar nicht eintreten kann. Was für den Hersteller neues Wartungsgeschäft bedeutet und dem Kunden geldwerte Vorteile bietet, ist unter IT-Sicherheitsgesichtspunkten der nächste Alptraum: gerade Fernwartungszugänge gelten als Achillesferse aller Steuerungscomputer[20].

Das nächste Einfallstor treiben Hersteller und IT-Industrie gemeinschaftlich voran. Im sogenannten „Internet der Dinge" wird den Produkten, mit Inbetriebnahme im lokalen Kontext, eine eigene Identität, sprich IP-Adresse, zugewiesen. Kleine Mess- und Funkchips in den alltäglichen Dingen, vom Kühlschrank bis zum Raumthermostat, vom Rauchmelder bis zum Türöffner, von der Toilette bis zum Auto, überall sollen jetzt funktional aufgebohrte Geräte über vermaschte Funknetze ihre Informationen weitergeben. Dabei hat noch keines dieser Geräte je einem Hackerversuch standgehalten[21].

Das Wirtschaftsministerium in NRW wiederum befürwortet eine Idee aus Kreisen der Wirtschaft, den Energieverbrauch der Ruhrindustrie als virtuellen Puffer zu nutzen, um die durch den wachsenden Anteil an Solar- und Windenergie auftretenden Strommengen- und Netzschwankungen zu stabilisieren. So könnte z.B. alleine die Essener Trimet AG binnen weniger Sekunden den äquivalenten Verbrauch einer Kleinstadt vom Netz nehmen, indem sie ihre Aluminiumschmelzwannen stromfrei schaltet. Diese Regelenergie, die max. acht Stunden zur Verfügung gestellt werden kann, ist vom Stromversorger auf vertraglicher Basis zu vergüten. Was energiewirtschaftlich im höchsten Maße wünschenswert erscheint, bleibt sicherheitstechnisch problematisch. Man male sich nur einmal aus, dass es einem Angreifer gelingt, eine Schadsoftware zu platzieren, die das Wiederanfahren der Schmelzen blockiert, die anschließend nur noch Schrott sind und das dieser Wurm über Jahre auf dem Rechner der Versorgers schlummert und erst im Ereignisfall überspringt bzw. aktiviert wird.

Niemand kann zum gegenwärtigen Zeitpunkt mit Sicherheit sagen, dass die kritische Infrastruktur in NRW gegen solche (und andere) Angriffsszenarien geschützt ist, noch dass das Netz frei von schlafenden Trojanern ist. Wer Wirtschaftsunternehmen ansiedeln oder auch nur halten will, der muss heutzutage nicht nur leistungsfähige Breitbandkabel anbieten (wobei NRW da nicht so schlecht dasteht) sondern auch und vor allem sichere IT-Strukturen. Was also ist zu tun?

[20] Berke, Jürgen: Geheime Mission. In: Wirtschaftswoche (2014) Nr. 31. S.44.

[21] Ries, Uli (2014): Hackerkonferenz:Cyberattacke aus dem Kühlschrank. In: http://www.spiegel.de/Netzwelt/web/defcon-konferenz-in-las-vegas-hacker-lieben-internet-der-dinge-a-985733.html (letzter Zugriff: 22.06.15)

Anfang der neunziger Jahre, als in ähnlicher Weise die Umwelt- und Klimadiskussion die öffentliche Wahrnehmung erreichte, hat das Land NRW das Wuppertal Institut als anwendungsorientierten Mittler zwischen Wissenschaft, Wirtschaft und Politik auf dem Gebiet des Klimawandels und der Ressourcenschonung aus der Taufe gehoben. Die gegenwärtig mehr als angespannte Haushaltslage und die 2020 einzuhaltende Schuldenbremse lassen es unwahrscheinlich erscheinen, dass NRW erneut zu einem solchen Kraftakt der Grundfinanzierung fähig ist. Wo Gelder fehlen, ist Pragmatismus und Kreativität gefragt.

Was hemmt uns, die Bürger_innen und die sie vertretende Regierung, die im Land vorhandenen Kräfte in einem Netzwerk der Ideen zu bündeln und ihnen eine Plattform zu bieten, auf der sie kollaborieren und sich wechselseitig stimulieren können? In Zusammenarbeit zwischen dem Wirtschafts- und dem Wissenschaftsministerium, den Hochschulen, der Industrie und der öffentlichen Verwaltung, wären nachstehende Maßnahmen eine erste Zwischenetappe auf dem langen Marsch.

1. Das Wirtschafts- und das Wissenschaftsministerium heben in einer gemeinsamen Initiative das „Virtuelle Cyberspace Institut NRW“ aus der Taufe. Darin vernetzen sich die in Sachen IT Sicherheit führenden Unternehmen aus der Region mit den wenigen Hochschulinstituten, die auf diesem Gebiet forschen und Expert_innen ausbilden.

2. Den Rahmen hierfür könnte ein kleines Generalsekretariat stecken, das zunächst nicht mehr machen muss, als z.B. zweimal im Jahr zu einem runden Tisch einzuladen und zwecks öffentlicher Wahrnehmung einen jährlichen Kongress für Pan-Europäische Sicherheitsfragen auszurichten (Call for Papers).

3. Das Wissenschaftsministerium wirkt auf die Hochschulen ein, IT-Sicherheit und/oder IT-Sicherheitsmanagement zu einem Pflichtfach zu machen. Der Ideen- und Methodik-Austausch zwischen den Lehrstühlen ist zu fördern und in geeigneter Form zu unterstützen.

4. In IT-Vertiefungsfächern sollte den Studierenden die Möglichkeit geboten werden, sich in kontrollierter Umgebung in die Techniken des „Weißen Hackens“ einzuarbeiten. Die talentiertesten Hackergruppen könnten in einem Landeswettbewerb ihre Champions ermitteln, gerade so, wie es bei der Roboter-WM oder beim Meilenrennen der Solarfahrzeuge bereits der Fall ist.

5. Das Wirtschaftsministerium wirkt auf die kritischen Industriesektoren ein und hilft ihnen bzw. ermuntert sie, die Robustheit ihrer IT-Infrastruktur durch zusätzliche „weiße Hackangriffe“ von außen zu ertüchtigen. Den Student_innen aus den hiesigen Hochschulen böten sich interessante Beschäftigungsperspektiven und die beteiligten Unternehmen wären besser geschützt.

6. Die Landesbehörden unterziehen sich der gleichen Prozedur und gehen mit gutem Beispiel voran. Sicherheit aus NRW, für NRW.

Herausgeber: Friedrich-Ebert-Stiftung, Managerkreis, Hiroshimastr. 17, 10785 Berlin | Ansprechpartner im Landesbüro Nordrhein-Westfalen der Friedrich-Ebert-Stiftung: Jochen Reeh-Schall, Godesberger Allee 149, 53170 Bonn | Weitere Informationen: www.managerkreis.de