Mehr Resilienz wagen – Kritische Infrastrukturen schützen mit Manuel Atug (AG KRITIS)

Lobeck: [0:02] Herzlich willkommen zu einer neuen Folge des Podcasts City Transformer, heute ohne Franz Reinhard Habbel, der gerade im Land unterwegs ist und Kommunen berät.

Lobeck: [0:12] Ich habe einen Gast in unserem virtuellen Studio: Manuel Atug von der AG KRITIS. Herzlich willkommen.

Atug: [0:19] Hallo.

Lobeck: [0:21] Ja, wir wollten heute eigentlich mit StudioLink aufnehmen, das hat aber irgendwie nicht geklappt. Jetzt versuchen wir es mal mit Riverside. Ich bin gespannt, ob wir das technisch noch lösen können. Wir sind ja noch auf der Suche nach Nicht-USA-Produkten, die uns trotzdem eine gute Podcast-Erfahrung ermöglichen. Wir bleiben auf jeden Fall dran und berichten darüber.

Lobeck: [0:40] Wir sprechen heute mal nicht über "Was gibt es Neues", weil wir direkt in das Gespräch mit Manuel Atug einsteigen wollten. In Episode 43 haben wir uns – vielleicht erinnern Sie sich – über den Anschlag auf die Strominfrastruktur in Berlin unterhalten, den Franz Reinhard Habbel selbst auch leidvoll miterleben musste, als er ein paar Tage ohne Strom und Heizung war. Bisher noch unbekannte Täter hatten im Januar eine Kabelbrücke am Heizkraftwerk Lichterfelde in Brand gesteckt und somit die Stromversorgung des Kraftwerks und von etwa 45.000 Haushalten und 2.200 Betrieben im Südwesten Berlins gekappt. In den Stadtteilen Nikolassee, Zehlendorf, Wannsee und Lichterfelde gingen dann die Lichter und Heizungen aus.

Lobeck: [1:28] Im Nachgang wurden dann von verschiedenen Seiten Forderungen laut, die es für eine gute Idee hielten, die offenen Daten und die Informationsfreiheit in Berlin ein bisschen einzuschränken, damit mögliche Täterinnen und Täter nicht auf irgendwelchen Karten oder in Dokumenten finden, wo die Stromleitungen liegen. Franz Reinhard Habbel und ich hatten schon spontan den Eindruck, dass das vielleicht keine gute Idee ist, dachten dann aber, wir fragen einfach mal jemanden, der sich mit kritischer Infrastruktur auskennt. Und da ich ihm auf Mastodon folge, bin ich auf Manuel Atug gekommen, der Gründer und Sprecher der AG KRITIS ist – ausgesprochen: AG Kritische Infrastrukturen. Das klingt jetzt wie eine Bundesbehörde, ist aber keine.

Lobeck: [2:15] Herr Atug, was ist die AG KRITIS und was ist Ihre Rolle dort?

Atug: [2:20] Ja, die AG KRITIS ist eine unabhängige Interessengemeinschaft. Wir sind also kein Verein, Verband oder was auch immer, sondern ein loser Zusammenschluss von Menschen, die mit kritischen Infrastrukturen viel zu tun haben und die gesagt haben: Mit Wissen kommt Verantwortung, und die wollen wir wahrnehmen. Wir vertreten also keine Interessen von Unternehmen, Wirtschaftsverbänden oder des Staates, sondern wir haben ein einziges Ziel: unabhängig kommunizieren zu können und die Versorgungssicherheit der Bevölkerung zu erhöhen. Dazu sind wir bis zu 42 Fachexpertinnen und Fachexperten, die täglich mit kritischen Infrastrukturen zu tun haben. Wir versuchen, aus dieser Motivation heraus die Verbesserung der IT-Sicherheit und der Prozessautomatisierung – also der Automatisierung in den Produktions- und Fertigungsanlagen – kooperativ mit allen Beteiligten herbeizuführen. Wir würden gerne dazu beitragen, dass entweder Großschadenslagen durch Cyber-Vorfälle in den kritischen Infrastrukturen gar nicht erst passieren, oder dass diese zumindest in ihren Auswirkungen reduziert werden und dass man die Krisen und Katastrophen, die dann eintreten, sinnvoll bewältigt.

Atug: [3:33] Ich selbst bin beruflich wie auch privat seit vielen Jahrzehnten mit dem Thema KRITIS befasst. Ich setze mich mit der EU-NIS-2-Richtlinie auseinander, habe mich auch mit NIS 1 und KRITIS selbst intensiv beschäftigt.

Atug: [3:52] Ich adressiere das KRITIS-Dachgesetz, das physische Sicherheit gegen Naturereignisse, Sabotage oder Vorsatzhandlungen generell und auch gegen Unfälle adressiert. Ich befasse mich aber auch mit den Themen Hackback, Ethik, Hybrid Warfare, Cyberresilienz und digitaler Katastrophenschutz, aber auch mit Bevölkerungs- und Katastrophenschutz – um zu sagen: Naja, wenn das alles nicht klappt, muss man da ja auch nochmal hingucken. Die AG KRITIS, aber auch ich selbst, wir beraten regelmäßig oder sind als Sachverständige in der Bundesregierung, im Bundestag oder auch bei den Bundesländern tätig, schreiben Stellungnahmen zu Gesetzen und stehen für Hintergrundgespräche zur Verfügung. Ich bin auch Experte der European Research Executive Agency, und da befassen wir uns immer wieder mit all diesen Bereichen rund um Cybersicherheit und Katastrophenschutz.

Lobeck: [4:43] Okay. Ja, ich erinnere mich auch: Ich habe im letzten Jahr auf der re:publica einen Talk von Ihnen gehört. Da sah das alles nicht so gut aus mit der Sicherheit, diesen Eindruck hatte ich zumindest. Aber darauf können wir vielleicht im Verlauf des Gesprächs noch zurückkommen. Jetzt würde ich erst nochmal zu Berlin kommen. Die AG KRITIS hat sich ja auch nach dem Anschlag in Berlin

geäußert, nachdem diese Vorschläge kamen, man müsse das jetzt alles irgendwie verstecken, so tun, als gäbe es das nicht, und die Leute verwirren.

Lobeck: [5:13] Was sind Ihre wichtigsten Punkte zu diesen Vorschlägen?

Atug: [5:18] Bevor diese Vorschläge zur Sprache kommen, muss man zuerst wissen, dass im Berliner Stromnetz das Problem eine althistorische Trennung war: Man hat keine Vermaschung, keine guten Übergänge von Brandenburg nach Berlin, und damit ist das Stromnetz sowieso schon etwas anfälliger. Dieses Problem kennt man seit der Wiedervereinigung sehr intensiv, hat es auch immer wieder im Senat besprochen, aber immer wieder nach hinten geschoben, weil es eben auch teuer ist, dieses Defizit zu beheben.

Atug: [5:50] Insofern reden wir von einem Problem, das jahrzehntealt ist und nie richtig adressiert wurde. Da kann also niemand sagen, das sei jetzt plötzlich neu und das habe man nicht gewusst. Auch die Diskussion über die Täterfrage als Ablenkungsmanöver war sehr müßig und anstrengend, weil gesagt wurde: Das waren jetzt linke Terroristen, die waren besonders links, sehr weit links, zu viel links. Das sind Extremisten – klar, das sind Menschen, die offensichtlich einen wirkungsvollen Angriff durchgeführt haben und auch wirklich stören wollten. Aber ob die jetzt links oder rechts oder im Kreis sind: Der Punkt ist, es war eine Vorsatzhandlung, und die hat funktioniert. Was wir zusätzlich haben, sind ja auch Naturereignisse und Unfälle. Man müsste eigentlich alle drei betrachten und eine Resilienz dafür hinbekommen. Stattdessen haben wir sehr ausführlich über die Täterfrage als Ablenkungsmanöver debattiert – oder über die Tennis- und anderen Sportgewohnheiten von bestimmten Leuten in Berlin.

Atug: [6:52] Wenn man jetzt zu dieser Geheimhaltung von KRITIS-Daten kommt – also dieses “Security by Obscurity”, Sicherheit durch Verschleierung –, dann muss man nur zwei Minuten darüber nachdenken und merkt sehr schnell einige Punkte, die nicht schlüssig sind, sondern teilweise sogar das Gegenteil bewirken. Erstens muss man festhalten: Stromnetztrassen, die öffentlich waren, sind bekannt. Und die werden auch nie wieder geheim. Diese Kabel verlegt man ja nicht woanders hin, denn die liegen im Boden und bleiben da auch. Man kann höchstens zukünftige Kabel geheim halten, aber die, die bekannt sind, sind überall kartografiert und sehr ausführlich sichtbar. Der zweite Punkt ist, dass diese zentralen Infrastrukturelemente auch ohne Plan ohne Probleme erkennbar sind: Hochspannungsmasten, Mobilfunkmasten, Umspannwerke, Trafostationen, Kabelbrücken, Flughäfen, Kraftwerke – das kann man alles sehen, wenn man vorbeigeht. Ja, man könnte jetzt 30 Meter hohe Mauern bauen, dann sieht man es vielleicht nicht mehr – wie dann ein Flugzeug landen soll, weiß ich allerdings nicht.

Ich hätte aber auch umgekehrt gesagt: Wenn ich eine 30 Meter hohe Mauer sehe, dann wird wohl dahinter etwas an kritischer Infrastruktur stehen. Und wenn die vorher schon da stand, was ja bei Kraftwerken seit Jahrzehnten der Fall ist, dann weiß ich auch, worum es geht. Also das ist hinfällig.

Atug: [8:12] Und es macht irgendwie auch keinen Sinn. Da muss man auch sagen: Wer gezielt Schaden anrichten will, benötigt kein offizielles Online-Register. Es ist ja nicht so, als würden Saboteure, die wirklich Schaden verursachen wollen, sagen: “Naja, wir gehen da jetzt mal hin, wir müssen online nachgucken. Das können wir nicht so richtig erkennen. Oh Gott, die haben auch noch Videokameras. Nee, dann lassen wir das jetzt mit dem Attentat und gehen Latte macchiato trinken.” So funktioniert es ja nicht mit Akteuren, die wirklich schädigen wollen. Dann haben wir die Situation, dass Tiefbauunternehmen einen einfachen Zugang zu Leitungsplänen brauchen, um keine versehentlichen Beschädigungen zu verursachen. Die brauchen natürlich einen Plan, um zu wissen, wo Trassen verlaufen und wo man kein Loch in die Tiefe gräbt.

Atug: [8:59] In der Versicherungssprache heißt das “Baggerbiss”, und das passiert dutzendfach pro Tag in Deutschland. Diese Baggerbisse passieren versehentlich, weil die Leute eben nicht in die Karten gucken. Wenn wir die jetzt geheim halten, dann haben wir paradoxerweise viel höhere Risiken, dass es versehentliche Beschädigungen gibt, als dass wir eine gezielte Beschädigung verhindern. Damit konterkarieren wir eigentlich den angestrebten Schutzzweck, dass eben keine Ausfälle passieren. Und zuletzt muss man auch sagen: Präzise Infrastrukturdaten sind auch nach Naturereignissen oder Großschadenslagen für Einsatzkräfte von erheblicher Bedeutung. Ein Technisches Hilfswerk, eine Feuerwehr, ein Rettungsdienst – die müssen alle in der Lage sein, beschädigte Leitungen finden zu können, damit eine Eigen- und Fremdgefährdung beurteilt werden kann. Einsatzkräfte, die nicht wissen, wo eine beschädigte Leitung ist, gefährden ihr eigenes Leben oder verzögern die Hilfe für die Betroffenen. All diese Problemlagen haben wir uns jetzt mit dieser Geheimhaltungstheorie frei Haus eingehandelt, statt zu sagen: Wir versuchen, resiliente Systeme zu bauen.

Lobeck: [10:13] Okay, also das finde ich die Hauptbotschaft, die auch bei mir angekommen ist: statt Obscurity sozusagen Resilienz über verschiedene Elemente. Das fand ich nochmal gut, weil – für den Alltagsverstand klingt das ja erstmal plausibel: Wenn ich nicht möchte, dass jemand etwas findet, dann verstecke ich es, und dann wird es wohl keiner finden. Aber Sie haben ja mehrere Punkte genannt, die dagegensprechen. Erstens sieht man es ohnehin draußen. Man kann es digital verstecken, aber draußen sieht man es trotzdem noch. Und wenn man es einmal

digital gezeigt hat, dann ist es auch da. Und es brauchen eben ganz viele Leute diese Information. Dann verstecken wir es vor einigen wenigen, aber eben auch vor den ganz vielen – oder machen es zumindest für die schwieriger. Das fand ich sehr nachvollziehbar. Es klingt ja auch ein bisschen wie dieser Open-Source-Gedanke: Wenn etwas öffentlich ist, dann kann man es auch kritisieren und verbessern. Das finde ich auch noch einen ganz spannenden Punkt. Wobei es bei Software nochmal anders ist, weil wir da auch mathematische Modelle haben, die das dann – in Anführungszeichen – von alleine schützen, also nicht von alleine, aber wenn man sie anwendet, schützen können. Eine Verschlüsselung zum Beispiel. Das ist hier schwieriger. Aber ich finde Ihre vier oder fünf Punkte, die Sie genannt haben, einfach sehr plausibel. Warum denken Sie denn, dass die bei den Leuten, die das fordern, nicht so richtig ankommen? Berlin hat ja jetzt tatsächlich auch noch das Informationsfreiheitsgesetz geändert – ich weiß nicht, ob es genau so heißt, vielleicht heißt es ein bisschen anders – und diese Sachen da herausgenommen. Irgendwie scheint das Argument bei denen nicht zu greifen.

Atug: [11:42] Also, Sie haben noch einen wichtigen Punkt eingebracht, der in diesem Zusammenhang auch erwähnenswert ist, nämlich die Transparenz. Wenn man diese Transparenz hat, wie bei Open Source, dann hat man die Möglichkeit hineinzuschauen – und dann hat man auch die Möglichkeit, etwas dagegen zu tun, wenn es da Defizite gibt. Das hat man bei proprietärer Software nicht. Und wenn ich diese Lagepläne oder auch die Informationen über kritische Infrastrukturen bis zu einem gewissen Grad öffentlich habe –

Atug: [12:08] – dann hat die Zivilgesellschaft, dann haben die Behörden, die Aufsichtsbehörden, alle die Möglichkeit festzustellen, ob es da erhebliche Defizite gibt, ob jemand schlampt oder ob etwas nicht so funktioniert, wie es soll. Denn diese Transparenz ist ein wesentliches Merkmal einer demokratischen Gesellschaft. Das Geheimhalten ist tendenziell eher etwas, was Diktaturen vorantreiben, um zu sagen: Kritisiere diesen Staat nicht. Da hat man eine Unterdrückung, damit genau diese Kritik nicht stattfindet. Insofern ist auch die Transparenz bei den kritischen Infrastrukturen bis zu einem gewissen Grad sehr essenziell, um eben festzustellen, ob da jemand geschludert hat. Mit der Transparenz konnte man feststellen, dass diese Kabelbrücke völlig unzureichend gesichert war, dass sie Tage vorher – also wirklich fünf oder sechs Tage vorher – sogar umgekippte Bauzäune drumherum hatte.

Atug: [13:00] Sodass Fahrradfahrer und auch Kinder durchspaziert oder durchgefahren sind und gespielt haben, weil es da überhaupt keine Schutzmaßnahmen gab – also gar keine Schutzmaßnahmen. Das ist ein bisschen

sehr transparent, aber es zeigt in dieser Transparenz eben auch, dass die Sicherheitsmaßnahmen – wenigstens die, die sie da hatten – null gegriffen haben, null ernst genommen wurden und das nicht adressiert wurde. Und diese Defizite können wir zukünftig nicht mehr feststellen, wenn die Daten geheim gehalten werden. Also insofern ein ganz wichtiger Punkt, definitiv. Warum das bei den verantwortlichen Akteuren nicht ankommt? Ich würde schon unterstellen, dass es definitiv ankommt und dass die ganz genau wissen, was das bedeutet.

Atug: [13:42] Ich war ja auch in einer RBB-Talkrunde mit Frau Giffey und habe da sehr konkret gefragt, warum diese Defizite selbst im Oktober letzten Jahres noch bekannt waren. Da hat man gesagt: Das sogenannte Business Continuity Management vom Stromnetzbetreiber ist unzureichend. Also: Wie könnt ihr eigentlich in einem Schadensfall eine schnelle Wiederherstellung sicherstellen? Wie können die resilienter werden? Wie machen die Krisenbewältigungsmanagement? Auch im Oktober letzten Jahres wurde das schon wieder diskutiert, wie so oft. Warum werden diese Gelder nicht bereitgestellt? Warum macht man diese Sicherheitsmaßnahmen nicht?

Atug: [14:19] Warum weiß man seit der Wende, dass da ein Defizit existiert, und kümmert sich schlicht nicht darum? Sie war ja schon in mehreren Rollen dafür verantwortlich und ist aktuell auch mitverantwortlich. Und sie hat natürlich das heruntergespult, was man als Politikerin so herunterspult: Wir investieren Hunderte von Millionen in die nächste Zukunft und sichern alles ab. Und by the way: Berlin braucht in den nächsten zehn Jahren doppelt so viel Energie wie jetzt, und deswegen müssen wir mehr Leitungen legen. Aha. Also man investiert mehr Geld für die doppelte Leitungskapazität und auch den doppelten Stromverbrauch. Da wird man hoffentlich dann auch möglichst alles resilient und sicher machen. Aber das heißt eben auch, dass nur ein Bruchteil dieser vielen Millionen, die sie angekündigt hat, tatsächlich in diese Sicherheitsmaßnahmen geht. Das meiste wird nämlich in diesen Ausbau gehen.

Atug: [15:12] So versuchen die natürlich das umzusetzen, was zwingend notwendig ist – und das, womit man keine Werbung machen kann, womit man keine Wiederwahl gewinnt, was Menschen auch durchaus schwer entgegennehmen. Diese ganzen präventiven Maßnahmen, bei denen vielleicht unter Umständen irgendwann jemand irgendetwas tun könnte: Wir brauchen jetzt Kita-Plätze, wir brauchen dies, wir brauchen das, wir brauchen Fahrradstraßen, wir brauchen noch mehr Autos.

Atug: [15:37] Jeder hat so seinen Bedarf, und jede hat ihren Bedarf. Und dann sind Präventivmaßnahmen natürlich nicht gerade das, was man gern hören will. Aber

man kann sich definitiv sicher sein, dass die Kosten, die man gerade hatte, deutlich höher waren als ein Sicherheitsinvest im Vorfeld. Diese ganzen Kosten sind jetzt da gewesen, und das Geld ist weg. Man hat nicht wirklich irgendwelche Mehrwerte an Resilienz oder Sicherheit geschaffen. Das Geld hätte man besser dort hineininvestiert.

Atug: [16:05] Insofern gibt es sowohl beim Oberbürgermeister als auch bei ihr und bei verschiedenen anderen Akteuren nicht das Defizit, dass sie nicht wüssten, worum es geht, sondern eher das Defizit, dass sie sich fragen: Ist das für mich politisch opportun? Salopp gesagt. Und da kommen wir eigentlich immer hin, wenn wir als AG KRITIS die Frage stellen, warum etwas ein Defizit und ein Problem gewesen ist: Wir kommen eigentlich immer bei zwei Dingen als Ursache an. Das eine ist Erlösmaximierung, weil jemand Profitgedanken hatte, und das andere ist Machtmissbrauch, weil man die Macht, die man hat, zum Missbrauch des eigenen Vorteils nutzt und nicht für die Rolle, in der man eigentlich ist. Das hat man im Ahrtal erlebt, wie auch bei verschiedenen anderen Sabotagehandlungen in der Vergangenheit. Man sieht das bei allen ausländischen Akteuren, man sieht es aber auch bei den inländischen Akteuren, die diese Macht in dem Sinne missbrauchen, dass sie ihre Verantwortung und ihre Rolle nicht angemessen wahrnehmen, sondern lieber ihr eigenes Interesse an einer Wiederwahl in den Vordergrund stellen.

Atug: [17:10] Erlösmaximierung: Wenn ich Hunderte Millionen investieren müsste, sie aber lieber in der eigenen Tasche lasse, dann ist das natürlich sehr interessant. Und wenn ich dann Intransparenz habe, dann sieht vielleicht auch nicht jeder, dass ich hier ein bisschen spare und da ein bisschen spare. So haben wir dann Defizite in der kritischen Infrastruktur, die wir auch Stand heute an anderen Stellen haben. Ein kurzes Beispiel noch, dann passt es auch: In der Wasserversorgung haben wir Notwasserbrunnen, in jeder Kommune – auch Berlin hat viele Notwasserbrunnen. Man kann das in der Kommune nachfragen, aber die sind nicht öffentlich benannt. Die Adressen der einzelnen Notwasser-Entnahmestellen sind nicht öffentlich bekannt, man kann aber nachfragen und bekommt die Liste. Das hat ein Politiker in Berlin mal gemacht und eine Riesentapete an Adressen bekommen. Wenn man dann nachguckt, ob die alle funktionsfähig sind, dann stellt man fest: Ungefähr die Hälfte funktioniert noch, die andere Hälfte ist außer Betrieb, weil sie nicht ordnungsgemäß gewartet und instand gehalten wird. Und wenn man dann nachfragt, dann heißt es: Ja, aber an den Standorten könnten ja Saboteure Dinge tun. Faktisch ist es aber doch so, dass sie die Standorte geheim halten, weil man sonst feststellt, dass jeder zweite defekt ist. Dann würde man sagen: Ja, und im Problemfall kann die Bevölkerung kein Wasser bekommen, weil es kaputt ist. Aber

diese Diskussion bleibt aus, weil es nicht öffentlich ist und man es nicht einsehen kann.

Lobeck: [18:35] Ja, das ist ganz interessant. Also der Punkt mit der Prävention: Damit gewinnt man keine Lorbeeren, sozusagen, im politischen Diskurs. Das finde ich eine spannende Frage, denn ich fände – zumindest wäre der Punkt: Wenn man es öffentlich machte, dann heißt das ja noch nicht, dass alle gleich sagen "Hurra, wir machen jetzt Prävention", aber dann kann man es zumindest diskutieren. Dann könnte die Öffentlichkeit sagen: Naja, vielleicht reicht uns auch die Hälfte – um bei dem Beispiel zu bleiben – vielleicht reicht uns die Hälfte der Trinkwasserbrunnen. Wenn die Gesellschaft das nach einer Diskussion entscheidet und diese Risikoaffinität haben möchte, dann wäre das vielleicht eine gute Sache – vielleicht aus Ihrer Sicht noch nicht, aber ich würde erstmal sagen: Gut, wenn man in Ruhe darüber diskutiert, alle möglichen Sachen anspricht und sagt "Wir wägen das ab", und dann sagt "Ja, wir machen diese Sicherheitssache nicht und jene nicht, die kostet so viel Geld, und stattdessen machen wir die Kindergärten" oder was weiß ich – dann hat man sozusagen einen breiten Konsens darüber. Dann kann man als Gesellschaft sagen: Wir wollen das so, wir wollen diese Sicherheit nicht schaffen.

Atug: [19:39] Aber das funktioniert nicht so ganz. In einem offenen Diskurs würde man das so erwarten. Das Problem ist, dass wir keinen einfachen, offenen, ehrlichen Diskurs haben, sondern dass etwa X – also das ehemalige Twitter – sehr faschistisch in eine Richtung getrieben wird, sodass das Populistische, Faschistische und Extremistische in den Forderungen nach vorne gebracht wird und nicht eine sachliche Diskussion. Wir haben eine AfD, die das ausbeutet und sagt: Blackouts und all diese Risiken und Ängste, dass die Regierung unfähig sei – das versuchen die für sich zu proklamieren. Wir haben Tichys Einblick, Nius und wie sie nicht alle heißen, die das natürlich gleich entsprechend zu belegen versuchen. Es gab ja auch die Falschmeldung, dass beispielsweise Tausende Notstromersatzanlagen in die Ukraine geschickt worden seien und jetzt plötzlich keine mehr in Berlin da seien. Absoluter Nonsens. Es sind natürlich einige in die Ukraine geschickt worden – nämlich die, die man wirklich ohne Probleme überproduzieren und bereitstellen kann. Es sind beispielsweise aus NRW Dutzende Notstromersatzanlagen innerhalb kürzester Zeit nach Berlin gebracht worden. Die hatten an der Stelle nicht das Defizit. Natürlich hat Berlin selbst einen Mangel an Notstromersatzgeräten und musste dann Amtshilfe in Anspruch nehmen. Da kann man insgesamt bei allen mehr aufstocken.

Atug: [21:02] Aber die Diskussion war nicht, ob man zu wenig Notstromersatzanlagen hat. Das wurde aber missbraucht, und dann haben sich

diese rechtsradikalen Wutbürger und faschistisch angehauchten Menschen wutentbrannt darüber geäußert und gesagt: Die kriegen hier im Ausland alles, und die Migranten kriegen alles, und wir müssen hier trocken ausgehen – was ja völlig nicht der Wahrheit entspricht. Wofür sogar das THW seit einigen Jahren ein VOST – ein Virtual Operations Support Team – ins Leben gerufen hat, das dann Social-Media-Analysen macht, um auch das Lagebild in einer Krise zu unterstützen: Was sind Fake-Debatten, die da stattfinden? Was sind Fake-Nummern oder Überlastungen, weil sie falsche Nummern angeben oder eben genau nicht die richtige? Eine Notrufnummer 112 funktioniert ja, aber wenn die dann sagen "Die Telefonnummer der Polizei ist folgende, ruft bitte da an, die Notfallnummer wäre kaputt" – das war im Ahrtal auch passiert –, dann ist natürlich die normale Nummer überlastet, denn die ist ja nicht so aufgebaut wie eine Notrufnummer. All diese Dinge passieren parallel zu einer solchen Debatte.

Atug: [22:12] Damals hat sich schon der Innenminister Seehofer hingestellt und gesagt: Naja, im Ahrtal – wir bräuchten jetzt Sirenen, damit Alarm funktioniert. Vorher hatte er gesagt: Die Debatte führen wir nicht, wir stellen mal so 80 Millionen bereit, dann können die Kommunen, wenn sie 300.000 Seiten Formular ausgefüllt haben, ein bisschen Geld bekommen – und dann war die Diskussion durch. Das war wirklich ein Tropfen auf den heißen Stein, wir reden nicht von viel Geld. Und nachdem dann mehr als 130 Menschen im Ahrtal gestorben waren, hat er sich gönnerhaft hingestellt und gesagt: Wir haben 80 Millionen bereitgestellt, damit es Sirenen gibt. Er hat nur vergessen, dass die schon seit drei Jahren abrufbereit waren und nicht wegen des Ahrtals. Also auch da sieht man wieder: Prävention – "there's no glory in prevention", sagt man im Englischen. Damit kann man nur schwer einen Blumentopf gewinnen. Wenn man aber seine Aufgabe wahrnimmt, kann man sie sinnvoll erfüllen. Im Nachhinein stellen sich aber leider viele hin und versuchen genau diese Art von Machtmissbrauch und Eigenprofilierung, um sich gönnerhaft zu präsentieren, obwohl das eigentlich überhaupt nicht angebracht ist.

Lobeck: [23:16] Ich finde jetzt den Punkt interessant, den Sie – wenn ich mich richtig erinnere, ich habe das jetzt nicht nochmal eins zu eins angeschaut – vor allem auf der re:publica angesprochen haben, wo Sie etwas umfangreicher auf die Gesamtlage eingegangen sind. Wie ist das denn in Deutschland umgesetzt? Wir hatten ja das Problem, dass die alte Bundesregierung die Umsetzung von NIS 2 nicht mehr so hinbekommen hat und auch beim KRITIS-Dachgesetz nicht mehr, sodass das alles nochmal ein bisschen verzögert wurde. Aber das mal kurz abgehakt, weil sie ja nicht von vornherein geplant hatten, nicht mehr so lange zu agieren: Wie würden Sie grundsätzlich die Lage einschätzen? Zu Berlin haben wir

jetzt ein paar Sachen gehört, aber wie schätzen Sie grundsätzlich die Lage der Sicherheit kritischer Infrastruktur in Deutschland ein? Jetzt ohne, dass wir vier Stunden reden, aber ein paar Punkte.

Atug: [24:15] Ja, vielleicht – wer will: Der re:publica-Vortrag ist frei verfügbar, den kann man nachschauen.

Lobeck: [24:20] Ja, ich verlinke den auch in den Shownotes.

Atug: [24:23] Genau. Und diverse dieser Vorträge halte ich ja regelmäßig, viele davon sind auch online verfügbar, und eigentlich ist es immer dasselbe, was ich erzähle. Was braucht man für echte Resilienz? Vor zehn Jahren brauchte man ein Backup und eine Wiederherstellung. Jetzt braucht man ein Backup und eine Wiederherstellung. In zehn Jahren wird man – naja – ein Backup und eine Wiederherstellung benötigen. Denn die Frage ist nicht, ob ein 16-Jähriger aus seinem Kinderzimmer, der ethisch noch nicht ganz ausgereift ist, mich angreift, oder ob es ein russischer Saboteur war oder doch ein durchgeknallter Amerikaner mit seinen faschistoiden Big-Tech-Freunden. Die Frage ist gar nicht, was von wem passiert, sondern wie ich mich darauf einstellen kann und wie ich die richtigen Maßnahmen habe. Und ganz oft sind es immer dieselben Maßnahmen, die helfen. Wenn man sich jetzt NIS 2 und das Dachgesetz anschaut: Die alte Regierung hatte beides auf den Weg gebracht, weil die EU eben auch vorgegeben hatte, dass das Ende 2024 da sein müsse.

Atug: [25:20] Sie haben es versucht, und dieselben Akteure, die laut geschrien hatten, dass das völlig unzureichend und desolat sei, haben es dann als neue Regierung exakt im gleichen Wortlaut abgestimmt und erklärt: Naja, mehr können wir ja nicht tun, das ist ja schon so viel, und man muss doch auch an die Wirtschaft denken. Und da ist genau das, was ich mit dieser Eigenprofilierung und dem Machtmissbrauch meine: Als Opposition hat man himmelhochjauchzend laut geschrien, dass es auf gar keinen Fall gehe, und jetzt als Regierung hat man genau dasselbe getan. Allein durch diese politische Taktik hat man zwei Jahre verschenkt, in denen man Leben hätte retten können – das muss man so sagen. NIS 2 ist Ende 2025 in Kraft getreten.

Atug: [26:12] Es hat noch diverse Defizite, gerade bei der Rechtsdurchsetzung. Die Beträge der Strafen sind zwar hoch – bis zu 10 Millionen Euro, 2 Prozent des globalen Jahresumsatzes –, aber die Rechtsdurchsetzung ist fraglich, weil das zuständige Amt, das Bundesamt für Sicherheit in der Informationstechnik, dafür exakt null weitere Stellen bekommen hat, um das Ganze zu stemmen.

Lobeck: [26:34] Nur ganz kurz, vielleicht können wir das auch nochmal kurz erläutern – ich denke gerade, vielleicht wissen es noch gar nicht alle: NIS 2 ist im Kern die europäische Vorgabe zur Sicherung gegenüber Angriffen im Cyberraum, sage ich jetzt mal so grob. Oder wie kann man es sagen?

Atug: [26:48] Ja, genau. Also der IT-Betrieb muss gegen Störungen grundsätzlicher Natur funktionieren. Das müssen nicht nur Angriffe sein – auch der besagte Baggerbiss kann ja zum Stromausfall und dann zum Ausfall der IT führen. Und wenn ich eine kritische Infrastruktur bin oder eine sogenannte besonders wichtige oder wichtige Einrichtung, dann muss ich das durchaus auch melden. So versucht man, die Cybersicherheit im europäischen Wirtschaftsraum zu erhöhen, weil man sagt: Die Dienstleistungen, die alle erbringen, erbringen sie oft auch für ein anderes Bundesland oder sogar für einen anderen Mitgliedstaat, und da möchte man ein gemeinsames Mindestsicherheitsniveau im Cyberraum haben. Denn so funktioniert das europäische Miteinander: Man sagt, wir haben einen guten Wettbewerb auf Augenhöhe, und dafür müssen alle bestimmte Mindeststandards erreichen. Das ist die Idee dahinter, und das hat man – naja – durchaus mit Defiziten, aber in die Wege geleitet. Wenn man sich das KRITIS-Dachgesetz anschaut: Das ist sehr löchrig und sehr, sehr schlimm. Das ist mit Abstand das gruseligste Gesetz, das die AG KRITIS gesehen hat. Wir haben seit 2018 viele, viele Gesetze interpretiert. Da muss man wirklich sagen: Selbst durch eine Arbeitsverweigerungshaltung im Innenministerium hat man vorsätzlich Menschenleben riskiert, weil man einfach gesagt hat:

Atug: [28:09] Wir überarbeiten die Stellungnahmen nicht, was das Gesetz angeht, wir lassen das einfach so – sollen die anderen auch einfach dieselbe Stellungnahme machen wie vorher, dann sparen sich alle Arbeit. Dieses KRITIS-Dachgesetz soll ja, wie gesagt, nicht den Cyberraum ergänzen, sondern physische Schutzmaßnahmen für die Produktionsanlagen kritischer Infrastrukturen schaffen – also gegen Naturereignisse, gegen Unfälle oder Vorsatzhandlungen wirken, und auch gegen so etwas wie eine Pandemie, also eine große gesundheitliche Lage. Und im Wesentlichen gibt es drei Defizite. Erstens ist der Geltungsbereich viel zu generisch und unklar und wird erst in den nächsten zwei, drei Jahren genauer umrissen. Zweitens sind die Anforderungen nicht genau definiert, sondern da steht drin: Naja, man soll so resilient werden, und dann klappt das auch. Aber dazu geben wir auch eine Verordnung heraus, die kommt dann so in ein paar Jahren, circa 2030, und dann weiß man ja, was man tun muss. Und drittens die Strafen: Bis kurz vor Verabschiedung des Gesetzes hat man 500.000 Euro als maximale Strafe vorgesehen. Dann hat man gesagt: Okay, das ist wirklich lächerlich, wir haben es auf eine Million verdoppelt. Wenn ich aber als Unternehmen mehrere Dutzend

Millionen investieren muss, um physische Sicherheit herzustellen, und meine Strafandrohung im allerschlimmsten Fall maximal eine Million Euro ist –

Atug: [29:33] – ja gut, dann ist der wirtschaftliche Anreiz nicht gegeben, und die Wirtschaft wird dann natürlich auch nicht sagen: Wir machen das. Also egal, wo man hinschaut: alles Verzögerung, Verschleierung, Relativierung, Verordnungen, die später kommen. Das ist eigentlich eine leere Hülle und kein wirkliches Gesetz.

Lobeck: [29:50] Ich erinnere mich noch, dass Sie aufgezählt haben, dass einige Bereiche – zumindest bei NIS 2, glaube ich – auch gar nicht eingeschlossen sind. Wir haben ja immer ein bisschen den Fokus auf Kommunen. Habe ich das richtig in Erinnerung, dass die Kommunen eigentlich gar nichts tun müssen, zumindest nach dem Gesetz?

Atug: [30:10] Ja, also aus EU- und deutscher Sicht sind Kommunen vogelfrei, denn sie sind irrelevant für das Bestehen einer Demokratie, eines Staates. Sie sind auch nicht kritische Infrastruktur – wobei man fairerweise sagen muss: In Deutschland hat man auch den Sektor Staat und Verwaltung definiert. Da hat man gesagt: Naja, die staatliche und verwaltungstechnische Funktionalität muss gewährleistet sein. Man hat also im NIS-2-Gesetz Bundeseinrichtungen in Teilen adressiert, in ganz kleinen Teilen Landeseinrichtungen, aber die Kommunen und Landkreise kommen null vor. Darüber hatte auch der IT-Planungsrat – also die Bundesländer und der Bund zusammen – beschlossen und gesagt: Wir empfehlen auf gar keinen Fall, die Kommunen und Landkreise aufzunehmen, weil …

Atug: [31:01] … ja, wir empfehlen, dass das keine gute Idee ist. Und wenn man dann ohne Begründung und hinter verschlossenen Türen mal unter vier Augen nachfragt, dann wird gesagt: Bist du wahnsinnig? Wer soll denn das zahlen? Wir haben ja circa 11.500 Kommunen und Landkreise. Ich hatte auch mal eine Zeit lang gesagt: Naja, die haben halt einen sehr großen Investitionsstau in der IT. Da hat mich aus einer Bundesbehörde jemand, der sehr hoch aufgehängt ist, zur Seite gezogen und gesagt: Du Hase, du kannst mit dieser Investitionsstau-Nummer nicht hausieren gehen. Das würde implizieren, dass jemals jemand investiert hat. Das gab es nicht. Also erweckt diesen Anschein bitte nicht. Es gibt keine Investition in so etwas, und insofern haben wir nicht einen Investitionsstau, sondern ein komplett bestehendes Defizit seit Jahrzehnten. Wenn man das mal 11.500 beheben will, dann reden wir nicht nur von einem Sonderetat von 100 Milliarden. Insofern habe ich aufgehört zu sagen, es sei ein Investitionsstau – sondern wir haben da schlicht nichts.

Atug: [32:03] Und das ist mit dem IT-Planungsrat nicht besser geworden, der gesagt hat: bloß nicht. Die alte wie auch die neue Regierung haben gesagt: Nö, nö, das machen wir lieber nicht. Und die Bundesländer sagen halt: Naja, das ist ja Föderalismus, die Kommunen sind ja total selbstständig aufgestellt, die können das alle, die müssen ja eigenständig sein, da wollen wir gar nicht reingrätschen und Vorgaben machen. Was sie immer zu erwähnen vergessen: Wenn man Vorgaben macht, muss man auch die Rechnung zahlen. Insofern hat niemand Lust, Kommunen Vorgaben zu machen. Und die Kommunen – das muss man auch wissen – die meisten der 11.500 haben unter 10.000 oder unter 20.000 Einwohnerinnen und Einwohner. Die können sich nicht eine Riesensicherheitsarchitektur überlegen, ob physisch oder digital. Die werden strukturiert und systematisch mit dem Problem alleingelassen. Und das ist ein Unding. Da sagen wir auch als AG KRITIS: Kann das bitte mal behoben werden? Aber das möchte keiner hören, weil das zu viel Investment ist und das niemand machen möchte.

Lobeck: [33:05] Jetzt beobachten wir aber auch immer wieder, dass kommunale Akteure durchaus gehackt werden. Wir hatten eine Weile lang einen Landkreis, der nicht erreichbar war. Wir haben immer wieder einzelne Fälle, wir haben auch kommunale Krankenhäuser und solche Dinge, die immer wieder unter Beschuss geraten. Liegt das jetzt daran – wie Sie gerade sagten –, dass diese Organisationen quasi zu klein sind und zu wenig Ressourcen haben, um etwas zu machen? Oder ist das quasi unausweichlich, auch wenn die mehr machen würden?

Atug: [33:39] Also, Jens Lange macht ja in seiner Freizeit die Webseite kommunaler-notbetrieb.de. Die ist sehr hilfreich, weil er alles kartografiert – mit Übersichtskarte, Zeitleiste, Kategorien und Text – und das sozusagen alles in seiner Freizeit dokumentiert, weil der Staat selbst diese Transparenz nicht schafft. Das ist aber wieder das Thema Transparenz. Da kann man regelmäßig nachlesen, dass diese Kommunen mit klassischen IT-Sicherheitsmaßnahmen überfordert sind. Die haben …

Atug: [34:10] … archäologisch wertvolle Systeme direkt am Internet laufen, statt sie gepatcht und aktuell zu halten und die Sicherheitslücken zu schließen. Die haben DDoS-Attacken – also einen Überlastungsangriff, bei dem Tausende Systeme gleichzeitig die Webseiten aufrufen, sodass das System in die Knie geht, weil es diese Last einfach nicht trägt. Das sind in der Regel Angriffe aus den 90ern, in den seltensten Fällen wirklich ernstzunehmende große Probleme mit aktuellen IT-Infrastrukturen und Lösungskonzepten. Aber Kommunen haben diese eben oftmals nicht. Dann gibt es da Fachverfahren, die teilweise 20, 30 Jahre alt sind, in

Excel 95 zusammengebastelt wurden, und nur der eine Sachbearbeiter oder die eine Sachbearbeiterin kann das bearbeiten. Da hat man dann noch einen Windows-95-Rechner mit Excel 95 darauf, und nur die eine Person kann es bedienen. Das merkt man, wenn man sagt “Können Sie das tun?” und die Antwort lautet: “Die Kollegin ist im Urlaub, in drei Wochen können wir das für Sie erledigen.” Dann wissen Sie genau: Es gibt keine Vertretung, es gibt niemand anderen, es gibt nur dieses eine System. Davon gibt es zuhauf.

Atug: [35:18] Die Kommunen selbst machen das Problem auch noch stärker, weil sie natürlich auch sagen: Es gibt ein modernes System, aber das können wir nicht benutzen. Wir müssten die Hardware austauschen, die Software austauschen, alles migrieren, die Leute neu ausbilden – die Ressourcen haben wir gar nicht. Und so kommt es dann, dass beispielsweise im Fachverfahren Friedhofsverwaltung ein Tool eingesetzt wird, das WinFried heißt: Windows-Friedhofsverwaltung. Dieser Name war vor 30 Jahren noch passend, inzwischen würde man sagen: Nee, danke. Die Software ist auch genauso alt oder sogar noch älter. Und die gibt es in einer aktuellen Fassung auf aktuellen Betriebssystemen – und dann werben die damit, dass es Windows-95- und Windows-98-kompatibel sei. Wir sorgen dafür, dass eure althistorischen Systeme immer noch laufen, weil die Kommunen das verlangen und weil auch die kommunalen IT-Betriebe sagen:

Atug: [36:12] Wir kriegen jede Menge Geld, aber naja, wir lassen das so laufen. Es ist ein in sich geschlossenes System eines veralteten und an vielen Stellen fast schon verrotteten archäologischen Konstrukts – nicht an allen Stellen, aber an vielen. Und das zu lösen würde ja heißen: Ich brauche Leute mit Know-how und Kenntnis, und die fehlen in den kleinen Kommunen oft. Diejenigen, die es in den größeren haben, sind völlig überlastet und haben zu viel zu tun. So kommt man aus dieser Spirale nicht heraus und kann nicht sagen: Ich investiere mal Ressourcen in eine modernere Architektur, die auch zukunftsfähig ist und damit vielleicht sogar digital souverän, weil sie auf offenen, freien Standards basiert. Dann kann ich auch selbstbestimmt meine IT betreiben. Stattdessen hängen die Kommunen sehr oft von den IT-Dienstleistern ab, weil die definieren, was sie betreiben – und weil sie ein knappes Stadtsäckel haben, sagen die: Lass es so, wie es ist. Wir zocken immer noch jede Menge ab, müssen nichts umkrempeln, ihr auch nicht, und dann machen wir mit dem alten System weiter. Das bringt natürlich mit sich, dass viele Sicherheitslücken existieren, wo man heutzutage sagen würde, das sei fast schon grob fahrlässig oder Vorsatz. Aber die Leute sind schlicht überfordert oder haben nicht die richtigen Ressourcen und Mittel an der Hand, und weder der Bund noch die Bundesländer agieren da in angemessener Form.

Lobeck: [37:37] Aber das heißt jetzt auch als Schlussfolgerung, dass man den Kommunen eigentlich wenig Ratschläge geben kann. Denn wenn die überfordert sind und die Ressourcen nicht haben,

Lobeck: [37:47] dann sind Ratschläge ja so ein bisschen Makulatur, die man sich an die Wand hängen kann. Aber dennoch – oder was würden Sie sagen: Gibt es so eine Handvoll Dinge, bei denen Sie denken: Ja okay, das könnte man auf jeden Fall schon mal machen? Wenn man jetzt sagt: Okay, ich sehe das ein, der Atug hat recht, wir müssen ein bisschen mehr tun – womit sollten die denn anfangen?

Atug: [38:07] Also, erstmal muss man sagen: Egal wie schlimm die Lage ist, man macht es ja nicht besser, wenn man nichts tut – sondern sie verschlechtert sich jedes Mal. Und man kann auch mit einfachen Mitteln schon ein bisschen etwas bewirken. Wenn man Jahrzehnte gebraucht hat, um zu diesem Zustand zu kommen, dann wird man auch nicht in zwei Tagen die Welt retten. Es dauert durchaus vielleicht Jahre, bis man in einen guten Zustand kommt. Nichtstun verschlechtert es auf jeden Fall. Und man kann mit einfachen Quick Wins und pragmatischen Mitteln einiges leisten, was zumindest schon mal die größten Baustellen wegnimmt. Als Erstes kann eine Kommune hingehen und sagen: Wir benennen jetzt jemanden als Ansprechpartnerin für Sicherheitsfragen – also einen Informationssicherheitsbeauftragten oder eine -beauftragte – und sagen erstmal: Hier ist jemand als Ansprechpartner da, ihr könnt euch an diese Person wenden. Und diese Person versucht erstmal zu sichten, was für Defizite wir haben, was das Problem überhaupt ist. Wenn ich niemanden benenne, dann passiert auch nichts. Das ist der wichtigste Schritt. Man muss da auch nicht jemanden neu einstellen oder sagen, dafür hat jetzt jemand 80 Prozent seiner Zeit. Es darf auch im Kleinen erstmal begonnen werden, und man macht Schritt für Schritt die einzelnen Gänge.

Atug: [39:21] Also, ich sage immer: Wie isst man einen Elefanten? Nicht am Stück, sondern scheibchenweise. Dann fange ich mit dieser einfachen, banalen Scheibe an, die kostet im schlimmsten Fall nicht viel, ich muss keine Ausschreibung machen, ich muss keinen Einkauf aktivieren, ich kann jemanden benennen – vielleicht sogar eine Person, die dazu Lust hat – und sagen: So, du bist Ansprechpartnerin für diese Fragen. Dann kann man natürlich die wichtigsten Problemlagen anschauen und sagen: Okay, was sind denn die Einfallstore? Die üblichen Einfallstore sind archäologische Systeme direkt am Internet. Können wir da die neuen Updates des Herstellers relativ zeitnah aufspielen und interne Systeme später, weil wir erstmal versuchen, den Schutz von außen abzudecken? Damit hat man auch schon mal eine Priorisierungsreihenfolge: Wenn wir schon mal an den Maschinen sitzen, dann priorisiert an denen, dann kriegen wir das

auch ein bisschen besser geschützt. Wenn ich einen Fernzugriff habe – also eine Fernadministration von außen aus dem Internet in das interne Netz der Stadt oder Kommune –, dann kann ich auch sagen: Diese Fernwartung oder Fernadministration bitte nur Zwei-Faktor- oder Multifaktor-authentifiziert.

Atug: [40:33] Fernwartung ist eines der gruseligsten Probleme, die man in der Wirtschaft, in den kritischen Infrastrukturen, aber natürlich auch in Kommunen findet. Das ist ein Einfallstor, das ist wirklich sehr einfach für Akteure – genauso wie ungepatchte Systeme direkt am Internet. Wenn man diese zwei Dinge schließt, hat man schon wahnsinnig viel Risiko reduziert. Wenn man dann noch Ressourcen hat, dann hilft es auch zu fragen: Was sind denn Maßnahmen, mit denen wir Phishing-Angriffe reduzieren können? Also ein sicheres Mailsystem, und es gibt zum Beispiel diese Konfigurationsoptionen, dass man sagt: Diese Mail kommt von außen und nicht von innen. Wenn also der Kollege oder die Kollegin mich anschreibt, aber da steht der Warnhinweis “Achtung, diese Mail kommt von außen”, dann weiß ich schon mal: Das ist nicht der Kollege oder die Kollegin. Das sind einfache technische Maßnahmen. Und natürlich kann man auch mit den Leuten reden und sagen:

Atug: [41:27] Okay, wir haben insgesamt eine schwierige IT-Lage, aber wie können wir einfache Sicherheit etablieren, wie können wir miteinander reden und uns austauschen? Das heißt, auch so etwas wie eine Organisationskultur, eine Kommunikationskultur – nicht hierarchisch und bloß nicht laut werden, wenn es Probleme gibt, sondern eine offene Kommunikationskultur. Die kann extrem helfen. Da muss ich noch nicht einmal Phishing-Kampagnen-Systeme kaufen, sondern ich versuche erstmal zu sagen: Wenn ihr Probleme seht oder ihr vermeintlich auf irgendetwas geklickt habt und denkt “Das ist jetzt komisch” –

Atug: [42:04] – dann ruft doch bitte die eine Person oder die Abteilung an, und die nehmen sich der Sache an. Und die gehen sogar dran und sagen: Oh, danke für den Hinweis, wir gucken sofort, weil das jetzt Prio hat. Und wenn es ein falscher Alarm war, sagen die: Trotzdem danke, hätte ja sein können. Also hast du richtig gehandelt, gut gemacht, beim nächsten Mal bitte wieder anrufen. Wenn man den Leuten aber sagt “Jetzt hast du wieder Ressourcen gefressen, und das war doch überhaupt nichts, warum meldest du dich?” – die rufen nie wieder an, die melden sich nicht. Mit dieser Organisations- und Kommunikationskultur kann ich also unheimlich viel bewirken, ohne auch nur einen Cent investiert zu haben. Einfach nur in der kulturellen Art und Weise, wie man miteinander umgeht. Und das sind jetzt schon vier, fünf Maßnahmen, die liegen eigentlich auf der Hand. Egal, wer es ist – ob eine Kommune, eine kritische Infrastruktur, ein Wirtschaftsunternehmen

oder eine Privatperson –, die sind eigentlich immer gültig. Aber bei Kommunen, wenn die diese Defizite haben, dann sollten die sich in dieser Reihenfolge um diese Sachen kümmern und sagen: Wenn wir das geschafft haben, haben wir schon einen Großteil der Baustellen, die richtig riskant sind,

Atug: [43:15] abgeschafft, und dann kommen wir langsam in eine stabile Seitenlage. Wenn man das geschafft hat und diese Erfolge sieht, kann man auch Stück für Stück langsam weitergehen und sagen: Dann gucken wir uns jetzt mal das interne System an, dann versuchen wir jetzt mal – diese Fachanwendung muss ja eh ausgetauscht werden – die als Open Source mit freien Standards auszuschreiben. Wie müssen wir das ausschreiben? Oh, da gab es doch von – keine Ahnung – DO-FOSS, Dortmund, irgendwie so einen Zusammenschluss, die haben doch mal irgendwelche Vorgaben geschrieben. Die sind ja frei verfügbar. Dann recherchieren wir mal oder sprechen mit den Kollegen aus den anderen Kommunen, vernetzen uns und besorgen uns sozusagen die Info, die wir nicht extra selbst erstellen müssen, sondern die schon alles da ist.

Atug: [44:02] ZenDiS ist übrigens auch eine Option, die man nutzen kann. Die bieten ja komplette, freie, Open-Source- und auf freien Standards basierende Arbeitsplatzumgebungen an und unterstützen Kommunen sogar bei der Einführung. Das kann man anfragen, man muss sich in die Reihe stellen, die haben leider auch zu wenig Leute und zu wenig Geld, weil dieser Open-Source-Gedanke und diese Resilienz in der Regierung anscheinend noch nicht so ganz angekommen sind. Aber auch da: Die haben schon – ich weiß gar nicht – 300.000, 400.000 oder inzwischen 500.000 Rechner in den Kommunen umstellen lassen. Man spart sich die Lizenzkosten und diese Abhängigkeit von den großen Big-Tech-Konzernen. Und das kann man wieder investieren in mehr Funktionalität, in Aktualität und in Sicherheit. Das muss gar nicht so kompliziert und aufgeregt sein. Man kann sich auch unaufgeregt da dransetzen und diese Schritte gehen. Das geht.

Lobeck: [44:54] Okay, das ist schon mal gut. Dann vielen Dank für die quasi einfachen Schritte, die Kommunen machen können – auch wenn es bei mir so ein bisschen ankommt, dass wir dafür trotzdem noch ein paar Jahre, vielleicht auch Jahrzehnte brauchen werden, um auf ein höheres Niveau zu kommen. Aber dennoch ist es richtig, genau wie Sie es sagen: Das beginnt mit dem ersten Schritt, und wenn man den nicht macht, wird alles schwieriger. Wir sind tatsächlich schon am Ende unserer Zeit angekommen, auch wenn ich noch viele Fragen hätte – aber das kann ja nochmal kommen, mal gucken. Herzlichen Dank für Ihre Einschätzung, sowohl zu Berlin und der Frage, ob man Dinge verschleiern sollte oder nicht, als

auch zur generellen Einschätzung, wie es um unsere kritische Infrastruktur und deren Sicherheit bestellt ist und was man vielleicht auch auf kommunaler Seite mit wenigen einfachen Schritten schon erreichen kann. Herr Atug, vielen Dank, machen Sie es gut. Und an die Hörerinnen und Hörer: Wenn Sie auch Themen haben, die Sie interessieren, dann schreiben Sie uns gerne eine Mail an info@habbelundlobeck.de, die erreicht uns beide. Und beim nächsten Mal haben Sie dann auch wieder Franz Reinhard Habbel dabei. Auf Wiederhören.

Atug: [46:02] Dankeschön, tschüss.