Folge 22: Sind wir gewappnet für den Krieg im Netz?

Sendung: Freitag, 20. Mai 2022
Autor: Dennis Kogel
Regie: Simone Halder
Redaktion Kugel und Niere: Christian Alt
Redaktion ZDF: Jens Monath, Heike Schmidt
Produktion: ZDF in Zusammenarbeit mit und Kugel und Niere

Atug: *Also Ransomware ist eine Software, über die in der Regel die Systeme verschlüsselt werden, oder die essentiellen Daten in den Systemen, sodass dann anschließend eine Lösegeldforderung gestellt wird und gesagt wird: Na ja, wenn ihr soundso viel bezahlt über eine Kryptowährung wie Bitcoin oder Monero, dann geben wir euch den Entschlüsselungsschlüssel und ihr könnt wieder an alles dran und könnt dann auch wieder arbeiten. Und wenn nicht, dann sind die Daten weg. Die haben aber dann realisiert, Privatpersonen stellen sich echt doof irgendwie Bitcoin zu besorgen. Und stellen sich auch doof …*

Lesch: Ich wüsste auch nicht, wo ich die herkriege.

Atug: *Das ist völlig normal. Viele Leute wissen es nicht. Ich wüsste es übrigens auch nicht. Ich müsste auch erst gucken, wie ich privat die bekomme.*

Lesch: Ich würde dich anrufen und sagen: Manuel, ich brauche Bitcoin, dann weißte Bescheid.

Atug: *Ich kenne Leute, die ich dann frage und dann kann ich das ganz schnell regeln, genau.*

Hallo, hier ist der Terra X-Podcast mit Harald Lesch. Heute habe ich mir einen Macher aus dem digitalen Maschinenraum Deutschlands eingeladen. Jemand, der hilft, wenn virtuell etwas schief geht und wie schnell das gehen kann, das haben wir erst neulich gesehen. In der Nacht vom 24. Februar hatten plötzlich sehr viele Menschen mit Satelliteninternet kein Netz mehr. Der Grund: Russland hat einen Satelliteninternetbetreiber so gehackt, dass dieser gefälschte Updates an zehntausende Modems verschickte. Die haben sich dann mehr oder weniger selbst zerstört und plötzlich konnte niemand mehr ins Internet. Und das hatte nicht nur Auswirkungen auf Privathaushalte. Mehr als tausend Windräder standen plötzlich still, weil sie eben auch über Satelliteninternet remote überwacht und gesteuert werden. Und in den letzten Tagen scheinen prorussische Hacker vermehrt Angriffe auf deutsche Behörden unternommen zu haben, unter anderem auf die hessische Polizei und das Bundesverteidigungsministerium. In unserer komplexen, ineinander verzahnten Welt können Störungen ungeahnte Konsequenzen haben. Und die Angst ist groß. Was ist, wenn Kriege in der Zukunft nicht mehr mit Bomben gewonnen werden, sondern mit gezielten Hacking-Attacken auf unsere kritischen Infrastrukturen? Und wie können wir unsere kritischen Infrastrukturen wie zum Beispiel Wasser, Stromversorgung überhaupt schützen? Über all das und mehr will ich mit meinem heutigen Gast sprechen. Manuel Atug. Manuel ist einer der gefragtesten Experten in Deutschland was Cyberwar und Cybercrime angeht. Er arbeitet seit über 23 Jahren in der IT-Sicherheit ist langjähriges Mitglied des Chaos Computer Clubs und Sprecher der AG Kritis, einem unabhängigen Experten-Panel, das sich sehr dafür einsetzt, kritische Infrastruktur besser vor Cyberangriffen zu schützen. Ich will mehr über die Gefahren, die von

Cyberangriffen ausgehen, wissen und ich kann jetzt schon versprechen: Manuel Atug hat eine gute Idee, wie man damit umgehen könnte. Da ist er ein Macher. Ein Macher, der seit ein paar Jahren mit voller Kraft eine Idee verfolgt, die einen gewaltigen Unterschied machen könnte. Aber erst einmal habe ich ein paar grundsätzliche Fragen an den Cyber Experten.

Lesch: Wie bist du denn zu dieser ganzen Sache gekommen? Wie wurdest du zu einem der gefragtesten IT-Security-Experten in Deutschland?

Atug: *Ich habe mich schon seit ich sechs bin an den Rechner gesetzt und habe mich immer darum interessiert, wie man den einsetzt, wie es eben nicht im Handbuch steht. Und hinter die Fassade gucken, dieser neugierige, spielerische Trieb mit der Technik, der war sozusagen integriert. Und ja, mit meinem Job, ich habe dann Informatik studiert und auch Lust und Laune gehabt an dem ganzen Digitalisierungsgeraffel. Und mit dem Job bin ich eben in Berührung gekommen mit kritischen Infrastrukturen, die ich eben beraten und geprüft hab. Oder auch vorher gepentestet.*

Lesch: Gepentestet?

Atug: *Also bewusst, da eingebrochen im Auftrag dieser Firmen und habe eben aufgezeigt, welche Lücken sie haben, sodass eben die Angreifer diese nutzen könnten. Missbräuchlich. Und jedes Mal, wenn ich dann etwas gepentestet habe oder in der Beratung gesehen habe, dass da große Defizite sind, in der Prüfung gesehen habe, dass Dinge nicht so funktionieren, wie sie funktionieren sollten idealerweise, ist halt immer so ein Stück mehr dazu geworden, dass ich gesagt habe, wir haben hier Defizite, die die kannst du ja gar nicht weg beraten.*

Lesch: Aber es gab doch unlängst so einen Angriff. Im Rahmen des Ukrainekriegs wurde ja die Nachricht lanciert, dass auch hier in Deutschland einige tausend Windräder davon betroffen waren. Was war denn das für ein Angriff?

Atug: *Das war der KA-Sat-Angriff. Und zwar ist über die Bodenstation eines Satellitenbetreibers eingedrungen worden über die verschlüsselte Fernzugriffsverbindung, VPN. Da hat man unsichere Passwörter und lange genutzte Zugänge missbraucht um da einzudringen, hat eine Manipulationen in der Verteilung so vorgenommen, dass ein Update an alle Satellitenmodems ausgerollt wurde. Insgesamt sind 30.000 Modems mit diesem Update versehen worden, was dazu geführt hat, dass das Modem in einen Fehlerzustand gegangen ist und nicht mehr einen Satelliten-Uplink aufbauen konnte. Also die wurden disconnected und waren offline. Das waren allein 5800 Windräder die dann disconnected waren. Fernzugriff, eine Fern Administration, also eine Steuerung von einem Leitstand war nicht mehr möglich. Die sind dann in einen sogenannten Automatic-Safety-Modus gegangen und haben gesagt: naja, solange die Windstärke bis maximal x ist, laufen sie weiter und sonst schalte ich halt sicherheitshalber ab.*

Hier grätsche ich mal kurz rein, weil hier ein paar Fachwörter gefallen sind. Pentest zum Beispiel. Das ist kurz für „Penetration Test“. Unternehmen und Institutionen rufen für einen Pentest Menschen wie Manuel Atug an und sagen: „Sag mal, willst du nicht mal bei mir einbrechen, um zu überprüfen, wie sicher mein System ist?“ Vermutlich hätte so ein Test bei den Windrädern ergeben: Ihr seid zwar sicher, aber wenn das Internet nicht funktioniert, geht hier gar nichts mehr. Ich erkläre das noch mal kurz: nach dem Hack haben sich die Modems selbst abgeschaltet und konnten remote nicht mehr erreicht werden. Windräder

sind aber so gebaut, dass sie, wenn sie keinen Kontakt zum Internet haben, in den Sicherheitsmodus gehen. Sie laufen zwar noch eine Zeit lang, aber bei stärkerem Wind schalten sie ab.

Hier möchte ich auch schon mal über einen Begriff sprechen, der später noch wichtig werden wird: Resilienz. Resilienz bedeutet Anpassungsfähigkeit. Systeme müssen so gebaut sein, dass sie nicht bei der ersten Störung ausfallen. Also Resilienz hat was damit zu tun, dass man sich durch Störungen nicht stören lässt. Aber in deutschen Konzernen und Institutionen herrscht oft die Einstellung: Wird ja schon nichts schiefgehen, oder? Und genau dagegen kämpft Manuel an. Manchmal durchaus, um im Bild zu bleiben, wie Don Quichote gegen Windmühlen. Aber zurück zu den Auswirkungen des Satelliten-Hacks zu Beginn des Ukrainekrieges.

Atug: *Was auch betroffen war und was kaum jemand mitbekommen hat, ist mehrere ELW 2. Ein Einsatzleitwagen 2 ist für mittlere bis große Katastrophen. Das ist ein roter LKW, wo hinten drin ein Lageführungssystem ist. Das heißt, die haben alle möglichen Kommunikationsmöglichkeiten da drin. Das ist ein mobiler Lageeinsatzraum, wo sich der Krisenstab in einer Katastrophe zusammensetzen kann. Und die haben natürlich als Fall-Back einen Satelliten-Uplink, um zu kommunizieren. Beispielsweise in so einem Szenario wie im Ahrtal, weil nach einer Flutkatastrophe stand ja keine Bodenstation mehr. Und diese Modems haben eben auch teilweise das Update runtergeladen und waren funktionsuntüchtig. Hätte es also noch mal so ein Ahrtalszenario gegeben, könnte man da nicht kommunizieren. Und dann gab es auch die Anweisung von Landesinnenministerien: Bitte die Geräte, die noch nicht angeschaltet wurden, auslassen. Wir wissen nicht, ob sie aktuell noch das Update ziehen. Das ist aber ein Kollateralschaden gewesen.*

Lesch: Der war gar nicht beabsichtigt?

Atug: *Der eigentliche Zweck war tatsächlich, das Militär und die Polizeibehörden in der Ukraine benutzen ja auch Satellitenkommunikation, und die wurde dann angegriffen. Man hat auch geschafft, eine halbe Stunde ungefähr auszusetzen, also nicht sehr lang. Offensichtlich wollte man ja einen dauerhaften Ausfall oder einen sehr langen Ausfall. Das heißt, für die halbe Stunde, die man geschafft hat, hat man aber diesen großen Kollateralschaden in ganz anderen Ländern bewirkt. Da sieht man, wie gefährlich offensive Angriffe eigentlich sind und wie wichtig stattdessen die Defensive ist.*

Lesch: Digitale Kriegsführung, ist da draußen der Krieg ausgebrochen? Was ist da los in diesem Cyberspace?

Atug: *Also ich glaube, als erstes müssen wir mal den Begriff Cyberwar, auseinandernehmen. Cyberwar simuliert ja den Begriff Cyberkrieg. Man kann also durch den Einsatz im digitalen Cyberspace einen Krieg führen oder gewinnen. Und das ist natürlich Blödsinn, der von irgendwelchen alten weißen Männern auf bunten Powerpoint-Folien erzählt wird, weil sie aus der Rüstungsindustrie kommen oder weil sie eben ethisch falsch abgebogen sind, aber IT-Produkte verkaufen wollen, um einen Krieg zu gewinnen. Die Realität sieht so aus, dass natürlich eine kinetische Wirkmittelkriegsführung, also Bomben und Waffen sozusagen, eingesetzt werden und damit natürlich auch Schäden provoziert werden, an kritischer Infrastruktur oder auch die Bevölkerung mitbetroffen wird. Über einen reinen Cyberangriff kann ich ja keinen Krieg gewinnen. Ich kann meinen politischen Willen oder meine andere Sicht nicht auf dieses Land adaptieren und*

das nachhaltig durchziehen. Dazu muss ich immer noch Bodentruppen nachschicken, die dann auch sicherstellen, dass meine Meinung da dauerhaft etabliert wird. Und das kriege ich eben in einem reinen Cyberkrieg nicht hin. Deswegen ist dieser Begriff eigentlich völliger Unsinn. Was man schon nutzt, ist der Hybrid Warfare, also der der Mix aus kinetischen Wirkmitteln und auch dem Cyberspace oder dem Cyberraum. Das ist dann sozusagen die, die hybride Kriegsführung in der Form, dass man sagt, Dinge wie Fake News oder Propaganda, die früher ja mit Flugzeugen abgeworfen wurde als Fluginfozettel, überträgt man jetzt in diesen Cyberraum als vierte Dimension, nach den Dimensionen Luft, Wasser und Boden; es gibt es sogar noch eine fünfte den Weltraum. Und diese Dimension Cyberspace benutzt man mit, um zu sagen: Jetzt können wir viel effizienter und skalierender all diese Fake News verbreiten, Informationsgewinnung betreiben und damit natürlich die Kriegsführung taktisch oder, oder strategisch unterstützen. Aber das ist eben was anderes als zu suggerieren, dass es einen Cyberkrieg gibt und da wird dann wirklich die Entscheidung gefällt.

Lesch: Also am Ende ist es so was wie Desinformationskampagnen, die einfach gefahren werden, oder die Propagandamaschinerie.

Atug: *Ja, oder die Informationsgewinnung. Dass man sagt, man ermittelt Informationen aus der Kriegsführung des Gegners oder versucht Datenbanken aufzumachen und da irgendwelche Informationen rauszuziehen. Das gehört natürlich auch in den sogenannten Information-Warfare.*

Lesch: Wenn du jetzt mal so auf das nicht vorhandene Schlachtfeld des Cyber-Krieges, den es ja nicht gibt, sondern wo eben unglaublich viele verschiedene,

also wahnsinnig viele Akteure da drin sind, dann gibt es für mich zwei ganz wesentliche Punkte. Erstens: Wer sind die Haupttreiber dieser Angriffsszenarien, die immer wieder stattfinden, das ist das eine. Und die andere Frage, oder ganz konkret: Sind das noch Menschen? Oder ist es bereits so, dass die ganze Angriffssituation oder ich will es mal Störungen nennen, du hast ja auf deinem auf deinem T-Shirt auch Resilience draufstehen. Also Resilienz heißt ja, wenn man resilient ist, dann lässt man sich durch Störungen nicht stören. Und Manuel macht übrigens genauso einen Eindruck, der lässt sich nicht stören, finde ich großartig. Also wenn du jetzt mal denkst, was ist das Algorithmen getrieben, was da passiert oder sind das immer noch Menschen? Was weiß man darüber?

Atug: *Zum Glück ist das noch nicht Algorithmen getrieben. Man versucht natürlich auch KI, also künstliche Intelligenz, in Lage- und Gefechtsführungssysteme zu integrieren, damit mehr Intelligenz einzubringen. Man hat auch schon Drohnen-Systeme, wo durch KI automatisierte Mechanismen sozusagen die Entscheidungen fällen sollen. Das heißt so eine Drohne als Lethal Autonomous Weapon System macht sozusagen einen Patrouillenflug und wenn eine bestimmte Mustererkennung zuschlägt, dann beispielsweise fliegt sie selbstständig auf dieses Muster zu, sieht aus wie ein Panzer oder so, und hat halt noch so eine kinetische Sprengladung da und greift dann dieses Ziel autonom an. Der Vorteil aus dem Militärischen ist, dass wenn man dem Ding halt sagt, flieg jetzt diese Patrouille und erkenne diese Muster und agiere dann eigenständig, dass wenn der Gegner selbst die Kommunikation unterbricht oder stört - es gibt ja keine Kommunikation mehr - das Ding hat jetzt einen Einsatzbefehl und führt den gnadenlos aus. Das heißt auch durch so eine Kommunikationsunterbrechung kann der Gegner eben nicht mehr agieren. Diese Teile der Automatisierung, ja Autonomie gibt es schon teilweise. Die andere Frage, wer sind denn die Treiber*

des Ganzen? Leider muss man sagen ganz oft die alten weißen Männer aus der Rüstungsindustrie, die eben bunte Powerpoint-Folien malen und sagen: Mit so einem Cyberkrieg kann man das total super machen und man hat keine Opfer, man muss den Hinterbliebenen nichts mehr erzählen. Man kann ein ganz sauberes, seziertes Angriffsziel auseinandernehmen und hat eine Störung, eine cyberphysische Auswirkung. Ich greife im Cyberraum an, dann fällt Strom oder Wasser aus und das ist total sauber und toll und ich kann zielgenau eine, das nennt man im Militär dann Sabotage kritischer Infrastrukturen, oder auch die sozusagen Störung der Bevölkerung oder Unsicherheit der Bevölkerung von Innen bewirken, weil sie eben dann auch nicht mehr ihrer Regierung oder ihrem Militär vertrauen. Und die versuchen natürlich, ihre Produkte zu verkaufen und zu erzählen, dass das so toll ist. Oder, du hast es ja gerade schon angebracht, diese Vernetzung bedeutet eben, dass es eine Komplexität und eine Interaktion gibt, die man nicht mehr überschauen kann. Das heißt, sie suggerieren, dass mit einem Cyberangriff ein sauberer und todesfreier Zustand entsteht. In Wirklichkeit sind diese Abhängigkeiten und Komplexitäten so vernetzt und so feinmaschig, dass niemand mehr auf dieser Welt wirklich sagen kann: Ich kann das ganze Risikolagebild erfassen und wenn wir an der Stelle diesen Angriff fahren, wird folgendes sozusagen in der Kettenreaktion passieren.

Die Kettenreaktionen, von denen Manuel hier spricht, erinnern mich ein bisschen an den Schmetterlingseffekt vom US-Mathematiker Edward Lawrence. Der hielt 1972 einen legendären Vortrag mit dem Titel: Kann der Schlag eines Schmetterlings in Brasilien einen Tornado in Texas auslösen? Bei Lawrence ging es um dynamische Systeme, Systeme, die immer im Wandel sind und sich dauernd gegenseitig beeinflussen. Diese Kettenreaktionen führen übrigens auch manchmal dazu, dass wir Angriffe überhaupt entdecken. Eine der größten Cyber Operation

aller Zeiten, Stuxnet, wurde nur zufällig entdeckt, weil sich Windows-Computer im Iran abgeschaltet hatten. Ein IT-Sicherheitsexperte hatte daraufhin einen Virus entdeckt, der nur ein Ziel hat: Die Zentrifugen von iranischen Urananreicherungsanlagen zerstören. Über Jahre haben sich iranische Nuklearforscher gefragt, warum ihre Zentrifugen sich selbst zerstörten. Stuxnet war die Antwort. Und unsere vernetzte digitale Welt ist das größte und komplexeste dynamische System, das wir jemals gebaut haben. Unter dieser Prämisse bewertet Manuel Atug auch die ständigen Forderungen nach sogenannten Hack Backs, also digitalen Gegenschlägen. Dazu hat er eine klare Meinung.

Lesch: Ich stelle mir das immer so [vor], also die Bundeswehr hat doch neulich, was heißt [es ist] schon ein paar Jahre her, eine neue Waffengattung eröffnet, ich glaube, es hieß Cyberwar oder Cyber-Aktivitäten, nennen wir es mal so. Was machen? Weißt du …, kannst du darüber was sagen? Gibt es tatsächlich solche militärischen Cyber-Abteilungen? Es gibt ja verschiedene Filme, die so was immer mal wieder thematisieren. Ist da was dran? Passiert so was?

Atug: *Also ja, das gibt es. In Deutschland ist es zum Beispiel so, es gibt ja den Kommando-Cyber-Informationsraum. Das ist ja die, die Gattung, die sozusagen die Dimension Cyberraum adressiert. Da sind 13.500 Soldatinnen darunter gestellt worden, in diese Armee, in diese Teilarmee. Die meisten davon machen IT-Betrieb und Absicherung der Systeme für die Bundeswehr. Aber es gibt eben auch beispielsweise das ZCO, das Zentrum Cyber Operation, und die sind dafür da, um im Cyberraum zu wirken. Zu wirken bedeutet eben, dass sie eindringen und eben aktiv handeln. Kinetische Wirkmittel sind ja Bomben oder eben Raketen und die sollen eben eine Cyber-Wirkung ausführen können. Das sind circa 100, 150*

Menschen. Die sind 2015 in Afghanistan im Einsatz gewesen im Rahmen eines NATO-Artikel Fünf Bündnisfalls. Da sind sie eben gerufen worden und es hieß: Könnt ihr in das afghanische Mobilfunknetz einbrechen digital und eine entführte Person, das Telefon von der orten? Wir wollen gucken, ob sie eben an der Person dran ist oder ob die Entführer sozusagen hier Beschiss an den Tag legen wollen. Und das hat eben das ZCO offensichtlich getan und ist da eingedrungen, hat den Standort bestimmt und man konnte dann eben diese entführte Person, ich glaube, man konnte sie retten oder man konnte sagen, ja, ist da. Das heißt, diese Fähigkeiten gibt es weltweit sowieso überall, in den USA, in Deutschland und auch im Zuge dieser ganzen Fähigkeiten bespricht man natürlich auch immer wieder Sicherheitslücken zu kennen, ausnutzbare Lücken ausnutzbar zu machen durch Schadsoftware oder durch, ich nenne sie mal digitale Waffen oder so, und durch, durch diese dann eben auch wirken zu können. Und diese Fähigkeit zu wirken im Cyberraum, ja, das haben inzwischen weit über 100 Staaten auf der Welt. In Deutschland gibt es auch, gerade schon erwähnt, ganz viele Akteure, ich nenne das immer das Cyber-Wimmelbild der Verantwortungsdiffusion.

Lesch: Ali Migutsch Wimmelbilder.

Atug: *Da gibt es natürlich auch viele Akteure und ja, die halten halt Sicherheitslücken zurück oder sagen, wir haben hier eine, eine Prozessmethodik, dass wir offensiv angreifen können. Und der Hack back, den du vorhin angesprochen hast, das ist ja noch mal etwas, wo dann vor allem Leute aus dem Innenministerium sagen, wir wollen einen Hack Back können, sprich wir wollen, wenn uns einer von diesem System angreift, wollen wir dieses System lahmlegen. Und das klingt halt toll. Und im ersten Affekt sagt man: Ja, ja, gut, von da kommt der Angriff, dann machen wir das kaputt. Tatsächlich ist es aber auch da so, Die*

Kollateralschäden kann man ja nicht bestimmen. Abgesehen davon muss man ja auch erst mal die Attribution machen können, das heißt eindeutig zuweisen, wer ist eigentlich der Akteur gewesen? Und kann ich dann auch wirklich mit Gewissheit sagen: Ich treffe diesen Akteur? Ja, und all diese Faktoren kommen zusammen mit dem Kollateralschaden und dem nicht kalkulierbaren Risiko. Das ist halt extrem komplex. Und die Wahrscheinlichkeit, dass ich eine, eine ich sag mal Wirkung entfalte, das auch wirklich kollateralschadenfrei das Ziel lahmlegt, das ist halt nicht trivial. Wenn das so wirklich trivial wäre, dann hätte Putin in seinem Angriffskrieg in der Ukraine wirklich alles erstmal weggecybert und anschließend hätte er dann seine Truppen hingeschickt.

Lesch: Aber ist es nicht erstaunlich, dass angesichts der Entwicklung, wo ja sagen wir mal, die Verwundbarkeit von komplexen Systemen wird ja immer offensichtlicher. Also man hört ja dann vor allen Dingen auch irgendwann: Oh, komplexe Systeme, die sind ja sehr empfindlich gegenüber Bedingungsveränderung. Wie du gerade sagst, du kannst nicht mehr genau sagen, wo läuft das eigentlich hin. Das nennt man ja in der Philosophie schwache Kausalität: dass eben alles am Anfang …kleinste Veränderungen führen eben nicht …, kleine Änderungen in den Ursachen führen eben nicht zu kleinen Änderungen bei den Wirkungen. Dann könnte man sie ja gut verordnen, sondern es fliegt auseinander. Und dann ist es aber für mich zum Beispiel ein Wunder, dass so ein Gebiet wie die Finanzwelt sich zum Beispiel auf Blockchain und Bitcoins oder andere Kryptowährungen einlässt, wo doch klar ist, dass der verschärfte Einsatz von noch mehr Komplexität eigentlich zu noch mehr Instabilität führen muss. Wie siehst du das? Wie stark ist der drive, immer weiter und weiter in die Digitalisierung zu gehen und weniger in die Sicherheit der Digitalisierung?

Atug: *Na ja, ich mache es mal an einem plakativen Beispiel fest. Wenn man kritische Infrastrukturbetreiberinnen fragt: warum digitalisiert ihr? Da kommen alle möglichen Antworten. Die einen sagen: Habe ich im Manager Magazin gelesen. Der nächste sagt: Auf dem Golfplatz mit dem anderen CIO besprochen. Der nächste sagt: Ja, aber wir machen auch Industrie 4.0. Der nächste sagt: Aber wir müssen doch digitalisieren. Der Nächste kommt an und sagt: Ja, ist dann günstiger oder wir können mehr produzieren. Und der einzig echte Grund, warum man digitalisieren sollte in kritischen Infrastrukturen, ist tatsächlich mehr produzieren, und zwar immer dann, wenn ich mit der analogen Produktion die Bevölkerung nicht mehr versorgen kann. Wenn ich also beispielsweise eine Stadt mit 500.000 Einwohnern versorgen muss, dann muss ich eben Frischwasser gewinnen können aus Frischwassergewinnungswerken oder Brunnen für 500.000 Menschen. Wenn ich eben ohne Automatisierung und damit Digitalisierung, weil Digitalisierung ist immer eine Automatisierung der Produktionsprozesse, wenn ich das eben nicht mehr hinbekomme in vertretbar, in analog, dann nehme ich Digitalisierung, Automatisierungunterstützung, um eben für 500.000 Menschen zu produzieren. Und wenn in der Stadt in fünf Jahren 600.000 leben, dann muss ich entsprechend wachsen und kann ja nicht sagen: Naja, bei euch kommt immer nur von zwölf bis Mittag Wasser raus und ansonsten müsst ihr halt sparen. So funktioniert ja eine Grundversorgung nicht. Aber viele stellen eben all diese Argumente in den Vordergrund, statt zu sagen: Das ist der tatsächlich einzige Grund, warum wir digitalisieren sollten.*

Lesch: Also letzten Endes geht es um so was, wie schnell reagieren zu können, schnell Zugriff zu haben und nicht nur das, sondern fünf haben wir 150.000 gehabt, jetzt haben wir 500.000. Das schaffen wir eigentlich analog mit den Zeitskalen einfach nicht.

Atug: *Eigentlich ist es noch nicht mal schnelle Reaktion, sondern eine beständige Reaktion. Und zwar eine voll umfassende. Ich kann ja nicht sagen, ich versorge jetzt nur die Hälfte. Ich kann auch nicht sagen, ich habe jetzt mal nicht in die Zukunft geguckt, wie jetzt die Einwohnerzahlen wachsen oder so. Wenn man sich kritische Infrastrukturen wirklich im Detail, in der Produktion, also in den operativen Technologien, in den Fabriken und Produktionswerken anschaut, dann sieht man oft Technologien oder Komponenten, die sind Jahrzehnte alt. Also die älteste Wasserpumpe, die ich in einem Wasserpumpenhaus gesehen habe, war ein Trümmer von fünf mal fünf Metern, riesengroß. Die war 70 Jahre alt. Also das war deutsche Ingenieurskunst, die ist unkaputtbar. Und ich würde auch einen Kasten Wasser darauf wetten, dass die noch 70 Jahre läuft. Und was hat man gemacht? Man hat ein paar Feld Sensoren drum herum gepackt, um zu sagen, nicht jeden Monat muss jetzt ein Fieldservice-Techniker vor Ort [sein[und guckt mal nach der Lage, sondern wir haben die Feldsensoren, die messen eben den Durchsatz. Und so weiter und so fort. Spart viele Fieldservice-Techniker und damit wird Wasser auch wieder bezahlbar und günstig. Muss man ja auch immer an die denken, die Hartz IV haben oder an der Armutsgrenze leben. Die sollen sich ja auch Wasser leisten können. Also macht diese Art der Automatisierung ja auch Sinn. Aber nicht wenn man die Sicherheit nicht mitdenkt und dann sagt na ja, komme ich so ein Pumpenhäuschen und kann diese Leitung manipulieren, bin ich direkt im zentralen System und kann alle manipulieren? Das wäre schlecht. Das soll ja nicht passieren. Die eigentliche Frage ist doch eine ganz andere, die die Bevölkerung eigentlich beantwortet haben will. Die Frage ist nämlich: Kommt morgen noch Strom und Wasser aus der Leitung, ja oder nein? Und wenn ich nicht klar und deutlich ja sagen kann, dann hat die Regierung ein Defizit in der Resilienz. Und dann muss sie das auch adressieren.*

Lesch: Wie ist das, würdest du sagen, es gibt so eine Hierarchie bei den kritischen Infrastrukturen? Also zum Beispiel es wird ja immer wieder auch davon gesprochen, dass Krankenhäuser angegriffen werden von irgendjemanden, weiß der Teufel warum. Würdest du sagen, es gibt da eine besonders verwundbare und das geht nach unten hin, wird es immer stabiler oder, oder sind die eigentlich alle gleich?

Atug: *Das muss man aus zwei Sichten betrachten. Aus der Sicht, was ist die kritischste kritische Infrastruktur, aber sie sind alle kritisch, deswegen kann man das jetzt eigentlich nur bedingt priorisieren. Das Allerkritischste ist tatsächlich Strom, denn ohne Strom geht gar nichts. So, danach kommt eben Telekommunikation, denn ohne Kommunikation kann ich mich auch nicht in einer Krise abstimmen. Wir haben ja gerade die ELW 2 gehabt. Ich kann mich nicht mehr mit versprengten Leuten synchronisieren. Ich kann nicht finden, wo mein Vater, mein Kind wo auch immer geblieben ist. Und natürlich können sich die Katastrophenschützer oder auch das Militär, um zu verteidigen, nicht koordinieren. Aber Telekommunikation funktioniert nur, wenn man Strom hat. Wenn Strom ausfällt, wird auch nach kurzer Zeit so was wie Wasser ausfallen oder eben auch die Kühlhäuser, sodass dann auch relativ schnell ein Mangel bei Essen entstehen wird, etc. Also die Kettenreaktion ist bei Strom am höchsten und am zweithöchsten bei Telekommunikation.*

Um es mal zusammenzufassen: Manuel Atug sagt, die Ängste vor Cyberwar-Attacken aus dem Ausland sind übertrieben. Zumindest die staatlichen Angriffe, denn hier sind Bomben auf Kraftwerke immer noch effektiver, als sich über Monate in deren Sicherheitssysteme zu hacken. Trotzdem wünschen sich einige

Politiker, dass eine zweistellige Milliardensumme aus dem angedachten 100 Milliarden Sondervermögen für die Bundeswehr in deren Cyberabwehr fließen soll.

Es gibt noch eine andere Angriffs Flanke und die ist im Moment viel bedrohlicher. Cybercrime. Stellen wir uns kurz vor: Es ist ein stinknormaler Dienstag im Juli. Sie kommen morgens in Ihr Büro, fahren den Rechner hoch und plötzlich geht nichts mehr. Sie kommen nicht mehr in ihr Benutzerkonto rein. Auch mit dem Handy lassen sich keine Emails mehr abrufen. Nichts mehr geht. Nada. Nothing. Rien. Das Problem ist nur, sie haben nicht irgendeinen Job. Sie arbeiten in einem Amt und plötzlich stehen auch bei Ihnen im Landkreis alle Räder still. Sozialhilfe, Bafög, Eltern- und Kindergeld kann nicht mehr ausgezahlt werden. Und alles nur, weil Hackerinnen und Hacker in ihre Behörde eingedrungen sind und 500.000 Euro Lösegeld verlangen, wenn alles wieder funktionieren soll. Das ist kein ausgedachtes Beispiel. Genau das ist letztes Jahr im Landkreis Anhalt-Bitterfeld passiert: Der erste Landkreis Deutschlands, der wegen eines Hacker-Angriffs den Katastrophenfall ausgerufen hat. Cybercrime ist ein riesiges Problem, vor dem wir in diesem Land stehen.

Atug: *Wenn man aus der Cybercrime-, also aus den und aus der organisierten Kriminalitätsecke wie Ransomware schaut, dann ist es tatsächlich so, dass es keine ganz speziellen Branchen gibt, die sie ausmachen. Sie gehen weltweit überall drauf und das ist Mittelstand, das sind Großkonzerne, Kommunen und Landkreise oder sogar die kommunalen Dienstleister. Die nehmen das, was angreifbar ist und wo eben sie auch sagen, vom Preisleistungsverhältnis können wir hier sehr effizient viel Geld machen. Das sind in einer gewissen Phase auch viele Krankenhäuser gewesen oder viel sowas wie Landkreise und Kommunen, weil da natürlich auch teilweise öffentlicher Dienst ist und da die Infrastruktur dann*

tendenziell auch mal ein bisschen schlechter dasteht, weil man eben auch schlechter zahlt. In Zeiten des Fachkräftemangels ist schlechter Zahlen natürlich ein Defizit. Aber es bringt auch nichts mehr zu zahlen. Damit verschiebt man das Problem ein Jahr oder zwei und hat dann wieder das Problem. Aber man geht halt überall hin, wo es Geld gibt.

Lesch: Lass uns doch einmal diese Sache mit der Ransomware mal klären. Was ist Ransomware, wie läuft so eine Attacke typischerweise ab? Vor allem, jetzt mal was für diejenigen, die möglicherweise schon betroffen sind, die wissen schon, wie es geht. Aber vielleicht vor allen Dingen für diejenigen, die eines Tages merken, wenn sie ihren Rechner anmachen: Ups, was ist denn da passiert? Und dann gibt es so glaube ich, ein paar goldene Regeln, da müssen wir mal drüber reden.

Atug: *Also Ransomware ist sozusagen eine Software, über die in der Regel die Systeme verschlüsselt werden oder die essentiellen Daten in den Systemen, so dass dann anschließend eine Lösegeldforderung gestellt wird und gesagt wird: Na ja, wenn ihr soundsoviel bezahlt über eine Kryptowährung wie Bitcoin oder Monero, dann geben wir euch den Entschlüsselungsschlüssel und da könnt ihr wieder an alles dran und könnt auch wieder arbeiten. Und wenn nicht, dann sind die Daten weg. Das war so der Beginn von Ransomware und inzwischen haben eben diese organisierten kriminellen Tätergruppierungen das ganze verfeinert und wollen natürlich den Anreiz des Zahlens erhöhen. Die haben dann angefangen zu sagen: Na erst zerstören wir die Backups und dann verschlüsseln wir alles, weil diejenigen, die Backups hatten, haben gesagt: Wir zahlen nicht. Dann gab es natürlich Leute, die haben gesagt: Ihr habt zwar die Backups zerstört und alles verschlüsselt, zahlen wir trotzdem nicht. Wir haben nämlich offline Backups und*

spielen wir dann halt wieder ein. Und die sagen dann: ist ja doof. Wir haben jetzt ganze Arbeit gehabt und kriegen keinen Profit. Also haben sie angefangen zu sagen sogenannte double extortion, wir ziehen erst Daten ab, ziehen also teilweise Gigabyte, Massendaten wirklich von den Systemen runter, was irgendwie kritisch aussieht. Und dann wird verschlüsselt. Also erst die Backups und dann die Systeme. Das heißt das ist immer ein Katz und Maus Spiel, wo die Tätergruppierungen eben immer professioneller und marktwirtschaftlich getrieben agieren. Und wir reden da von einem Markt, Ransomware, ist so im Bereich mehrere 100 Millionen Dollar pro Jahr und das ist der Umsatz und der Umsatz ist ungefähr der Gewinn, weil Sie zahlen keine Steuern. Das ist eine sehr hohe intrinsische Motivation, sehr effektiv zu agieren und eben bei Maßnahmen Gegenmaßnahmen zu entscheiden. Und das funktioniert seit vielen Jahren sehr, sehr gut und deswegen sind diese Gruppen sehr ausgefeilt. Also als Privatpersonen hat man ja eher nicht mehr das Risiko, das passiert nur noch vereinzelt. Anfangs war das tatsächlich so, die haben im Streuschuss jeden verschlüsselt, den sie erwischt haben. Die haben aber dann realisiert, Privatpersonen stellen sich echt doof, irgendwie Bitcoin zu besorgen. Und stellen sich auch doof …

Lesch: Ich wüsste auch nicht, wo ich die herkriege.

Atug: *Ja, das ist völlig normal. Viele Leute wissen es nicht. Ich wüsste es übrigens auch nicht. Ich musste auch erst gucken, wie Private da rankämen.*

Lesch: Ich würde dich anrufen und sagen: Manuel, ich brauche Bitcoin. Dann weißt du Bescheid.

Atug: *Ich kenne Leute, die ich dann frage und dann kann ich das ganz schnell regeln.*

Lesch: Also ich erinnere mich an einen brutalen Angriff auf die Uni in Gießen, die also Gott sei Dank wegen einem Mitarbeiter noch gerade so abgebogen ist nach rechts. Aber dann dieser knackige Hacker-Angriff auf den Landkreis Bitterfeld im Sommer 2021, was war denn da los?

Atug: *Ja, Anhalt-Bitterfeld wurde von der Ransomware Tätergruppierung „Grief or die“ kompromittiert. Und die haben eben mehrere tausend Systeme von denen wirklich verschlüsselt. Und zwar, ich glaube, es war sogar übers Wochenende in Seelenruhe. Und nach diesem Angriff war nur noch funktional die Telefonanlage. Ich hab's zwar nie ermittelt, aber. Ich würde mal behaupten, dass es eine analoge Anlage und deswegen ist die noch in Betrieb gewesen. Das heißt die Mitarbeiterinnen kamen halt da hin und haben eben so eine Meldung auf dem Bildschirm gesehen: „Grief or die. You're fucked. Please pay“. Und dann stand da, ich weiß gar nicht, ob es eine Bitcoin- oder Monero-Adresse und "bitte kontaktieren Sie hier unseren Support Chat und dann können wir mit euch abstimmen, wie ihr die Kryptowährung kauft und wie viel ihr zahlen müsst". Die Forderung war 500.000 Dollar und die gesamten Systeme waren halt verschlüsselt. Kein einziges der 159 Fachverfahren wie Personalausweis beantragen, KFZ anmelden, Sozialabgaben, oder Sozialgelder auszahlen. Ging halt alles nicht mehr, weil sämtliche Rechner und Server waren verschlüsselt. Das war erstmal die Situation bei denen.*

Lesch: Was ist denn da passiert? Ich meine, ist das ein ganz normaler Landkreis, oder ist das ein besonders verwundbarer Landkreis gewesen, oder?

Atug: *Das war ein Landkreis wie jeder andere, der halt mehr oder weniger IT-Sicherheit umgesetzt hat und mehr oder weniger IT-Mitarbeiter*innen hat. Und wenn man halt als Ziel auserkoren wurde und eine Tätergruppierung sagt du bist jetzt VIP-Kunde, dann ja.*

Cybercrime inzwischen Big Business und viele wissen gar nicht, dass sie vielleicht ein offenes Tor ins Internet haben, durch das Angreifer und Angreiferin kommen könnten. Vor kurzem hat mir ein Freund zum Beispiel eine Website gezeigt, eine Art Google für Geräte, die am Netz hängen. Das sind zum Beispiel mehr als 12.000 offene Webcams drin. Das ist wirklich gruselig.

Lesch: Also da ist noch eine Sache, da muss ich auch nochmal fragen. Ich habe diese Suchmaschine Shodan kennen gelernt. Wie gut, dass ich so ein angenehmer Zeitgenosse bin und mir nicht irgendwelche Gedanken mache. Was ist das? Erzähl du doch mal, was, was macht Shodan?

Atug: *Also Shodan ist eine Suchmaschine. Die scannen den ganzen Tag lang alle Systeme im Internet. Die versuchen einfach brutal alle IP-Adressen aus. Alle Systeme sind am Netz angebunden über eine IP-Adresse und dann über verschiedene Ports, bedienen die eben verschiedene Dienste: E-Mail, Web und so weiter. Und die gucken einfach andauernd im gesamten Adressraum sozusagen. Was findet man wo? Und welche Antwort kommt dann zurück? Und dann kann man eben über Shodan sehr strukturiert sehen, was für Schwachstellen offenbar in diesem System existieren. Und die, da sie wirklich alles scannen, einfach stupide alles, erkennen sie eben nicht nur die offensichtlichen Webserver oder Onlineshops oder so, sondern eben auch Prozess- und*

Produktionssteuerungsautomatisierungskomponenten, also Industriesteueranlagen. Und die sind da genauso vertreten und die kann man da natürlich finden, wenn man die richtige Suche eingibt und teilweise haben die dann eben auch Lücken, die dann da aufgezeigt werden. Und darüber kann ich natürlich sehr strukturiert auch suchen, wenn ich eine bestimmte Branche oder einen bestimmten Sektor adressieren will oder eine bestimmte Schwachstelle, dann kann ich genau diese raus selektieren oder eine bestimmte Bezeichnung, die immer vorkommt. Siematik, dann weiß ich, es ist eine Siemens Siematik Prozesssteuerungskomponente. Und dann wirft er mir halt alle Siematik Systeme raus, die er gefunden hat und dann sage ich: Oh wunderbar, dann sehe ich sogar noch: Ach die steht in Deutschland, die steht in den USA und die hier auch noch mal in Deutschland. Ich selektiere jetzt nur noch die in Deutschland, weil ich will ja den Deutschen auf den Keks gehen, und dann kann ich das immer feiner selektieren und habe anschließend ein wunderschön kuratiertes Ergebnis. Genauso wie ich eben bei einer beliebigen Suchmaschinensuche, ja immer verfeinern kann nach was ich genau suche. Und das funktioniert eben für Systeme im Internet plus ihre Schwachstellen auf der Ebene.

Lesch: Also ich muss ja sagen, ich bewundere dich, dass du darüber so sprechen kannst. Ich bin sprachlos, also ganz ehrlich gesagt. Wie ich davon gehört habe zum ersten Mal, habe ich gedacht: Das gibt doch nicht, das kann doch nicht wahr sein. Also selbst ordentliche Bankräuber müssen also erst mal rausfinden, wann macht die Bank auf? Wo ist der Tresor? Und so weiter. Aber hier hast du Shodan, da kannst du alle diese Informationen kriegen. Und je nachdem, welches Kriminalitätspotenzial in dir steckt und du die entsprechenden Instrumente zur Verfügung hast, kannst du damit Dinge tun. Sind die denn wahnsinnig? Oder andersrum gesagt, ist den Leuten im Netz klar, dass es Shodan gibt und dass man

damit unter Umständen auch gefunden werden kann und die entsprechenden Lücken gefunden werden können. Guckt euch das an, Shodan. Übrigens, als Manuel eben gesprochen hat, ihr hättet mal mein Gesicht sehen sollen. Ich habe es ja nicht gesehen, ich habe es nur gespürt, weil mir ist einfach die Klappe runtergefallen. Ich habe nur ein bisschen was davon gewusst, aber als er es eben erzählt, da wurde es mir echt anders. Muss ich ganz, ganz ehrlich sagen. Also man braucht immer Hacker zu sein, um all diese Dinge herauszufinden. Webcams, Thermostate, alles drin.

Atug: *Alles drin. Aber man muss zwei Dinge unterscheiden. Das eine ist natürlich: Nein, die Menschheit weiß nicht, dass das existiert und weiß auch nicht es zu bedienen. Viele, die sozusagen aus der Sicherheitsbranche kommen, kennen es natürlich, weil es das Werk ist, sozusagen was man nutzen kann. Es gibt viele solche ähnlichen, vergleichbare Systeme, die man natürlich zum Guten wie zum Schlechten nutzen kann. Das ist das sogenannte dual use ja. Ich kann das natürlich auch nutzen, um zu sagen, ich bin kritische Infrastruktur-Betreiber*in und gucke jetzt mal, welche Komponenten von mir denn da offenbar gefunden wurden. Wenn ich halt 300 Standorte hab und, und 50.000 Systeme, dann ist das nicht mehr so trivial. Und dann kann ich das natürlich zum Guten nutzen und sagen: Oho, da stehen ja fünf Systeme drin, die müssen wir jetzt mal dringend überprüfen. Ist das wahr? Und wenn ja, was müssen wir tun? Der andere Punkt, der ganz entscheidend ist: Diese Informationen stehen offen im Netz. Die haben die nur kuratiert und zusammengesucht. Die stehen auch ohne Shodan offen im Netz. All diese Information kann ich frei zusammensuchen. Und was Shodan nur gemacht hat, ist das zu vereinfachen, weil sie es schon für mich getan haben. Das heißt, lange bevor es Shodan gab, habe ich ja genauso Informationen im Netz recherchiert, um zum Beispiel die Pentests oder die Audits vorzubereiten, die ich*

gemacht habe und gesagt, ich recherchiere jetzt ein bisschen. Das ist, ich sag mal so, man kann journalistisch gute und hochwertige Recherche machen, dann bin ich auf dem Niveau Shodan und kann das selber zusammensuchen, kann auch flapsig suchen und sagen, habe ich da so ein Ding im Netz? Nee, sieht nicht so aus, dann lege ich mich wieder schlafen und so wird teilweise kritische Infrastruktur betrieben. Mal so, mal so.

Lesch: Aber es ist natürlich so, dass durch Shodan die Anzahl derjenigen, die irgendwas finden können, natürlich enorm vergrößert worden ist. Denn wenn man das alles selber suchen muss, wenn man das alles recherchieren muss, das ist schon Arbeit. Und Shodan hat praktisch da schon Vorarbeit geleistet, die ja ganz erheblich sein kann.

Atug: *Ja, aber, da gibt es natürlich auch ein Aber. Es vereinfacht das natürlich für diejenigen, die nicht ganz so kompetent sind oder ganz so viel Ahnung haben oder für die, die faul sind. Das heißt, man unterscheidet ja auch die Angreifer und das ist immer wichtig: Wer ist der Akteur und was ist seine Motivation und was ist sein Ziel? Wenn man jetzt sagt, der Angreifer ist Putins Militär, das Ziel ist Ukraine und sie wollen nachhaltig Infrastruktur zerstören, dann werden die sich ja zweimal überlegen Machen wir ein Cyber-Angriff, benutzen wir Shodan oder werfen wir eine Bombe drauf? Bisher haben wir gesehen Variante drei war so die zielführende. Wenn es eben ein, ich sag mal ethisch nicht korrekter Hacker ist, oder eine, eine Tätergruppierung, die wegen Geld, Ransomware oder so, da vorgeht, kann die da natürlich reinschauen und sagen dann gucken wir uns das an. Eine Ransomware-Bande, die hoch kriminell und sehr organisiert und strukturiert ist, die wird auch ohne Shodan trotzdem weiterarbeiten. Die halten wir nicht ab. Die sind aber tatsächlich die, die uns sehr viel Schmerzen bereiten. Feld-, Wald-, Wiesen-,*

*Möchtegern-Hacker*innen die irgendwie, ich sage jetzt mal Script Kiddies sozusagen sind, die können Skripte bedienen, aber nicht programmieren. Die wissen auch nicht, wo und was man findet. Wenn doch, dann probieren die einfach alles aus. Ja, die schaffen es dann eher mal mit Shodan was zu tun als ohne. Ohne gibt es die auch oder trotzdem, die machen dann andere Dinge oder finden vielleicht mal so ein System und nerven uns dann trotzdem, mit Shodan wird es für diese Art von Kompetenzträgern, also eher untere Liga, etwas einfacher. Aber, gefühlt sind die Script Kiddies eher ein Grundrauschen im Internet. Das sollte einem ernsthaften Betreiber einer kritischen Infrastruktur nicht wehtun. Das wäre fatal. Und die hochkriminellen und strukturierten Akteure, das sind die interessanten und denen es egal ob Shodan da ist. Das heißt „security through obscurity", also durch Verschleierung oder Geheimhalten, funktioniert nicht und Shodan nutzt genau dieses Element und sagt: Diese Informationen sind öffentlich verfügbar. Wir zeigen sie euch, damit sie euch wehtun oder damit ihr euch schützt. Man kann es aber natürlich auch in die andere Richtung nutzen.*

Lesch: Manuel, der ist einfach derjenige, der selbst sprachlose Gesprächspartner einfach wieder sozusagen belebt, indem er sagt: Harry, halt den Ball flach. Ist alles gut.

Atug: *Es gibt noch Hoffnung.*

Lesch: Das ist wunderbar.

Manuel ist ein Typ, der macht Hoffnung. Vor allen Dingen, weil er nicht nur die Probleme genau sieht, sie präzise beschreiben kann, sondern auch was dagegen unternimmt. Denn hier wird aus dem Experten Manuel Atug ein Macher. Seit ein

paar Jahren verfolgt er konsequent eine Idee. Er glaubt, wir brauchen nicht nur ein Technisches Hilfswerk in Deutschland, das in Katastrophensituationen hilft. Wir brauchen auch ein Cyber Hilfswerk, eine Truppe von freiwilligen Helferinnen und Helfern, die dann ausrücken, wenn die Cyber Katastrophe da ist, wenn sie passiert ist. Weil die Gründung einer solchen Organisation rechtlich etwas komplizierter ist als die Gründung eines Vereins, ist das Cyber Hilfswerk, kurz CHW, bisher nur eine Idee. Ich wollte von Manuel wissen, was war der Auslöser für die Idee des Cyber Hilfswerks?

Atug: *Und dann kam irgendwann ein Gespräch auf der C-Base, das ist ein Hacker Space in Berlin, wo wir dann zu dritt dasaßen und haben irgendwie bei einem Kaltgetränk diskutiert und gesagt: Naja, was passiert denn, wenn die digitalen Bitwerte umkippen? Wenn Einsen Nullen werden. Ja dann kommt, ja wer kommt da eigentlich? Ach so warte, THW ist ja eigentlich nur für so analoge Schäden. Wer macht das denn im Cyberbereich? Ja doch warte, das BSI, das Bundesamt für Sicherheit in der Informationstechnik, die haben ja sogenannte MIRT, also Mobile Incident Response Teams. Wenn also was passiert, rücken die aus und helfen den Leuten vor Ort. Ja super, dann haben wir ja gesichert, alles jut. Aber wie viele haben die denn? So viele können das doch gar nicht sein, es gibt ja voll viele kritische Infrastrukturen. Dann haben wir halt geguckt und gesagt, das sind so um die 15 Leute, die haben noch Zugriff auf so circa 15 weitere, macht, so summa summarum brutto 30. Dann haben die Urlaub, Schichtdienst, sind mal krank, ein bisschen mau für Deutschland. Das war so die Grundidee, wo wir gesagt haben, aber eigentlich könnten wir doch helfen. Also, so wie beim THW: Ehrenamtler*innen, die einfach sagen, da sind Bitwerte umgekippt, dann helfen euch die aufzuheben. Wir haben ja ein Interesse daran, selber Strom und Wasser noch zu kriegen aus der Leitung und für unsere Kinder auch. Also liegt doch alles*

auf der Hand. Alles klar. Und damit war dann geboren die Idee, wir wollen eigentlich ehrenamtlich chillen, helfen, weiter chillen. CHW haben wir gesagt, kann man es jetzt nicht nennen. Naja, aber THW gibt es ja auch. Also Cyber Hilfswerk.

Lesch: Es ist ja wie bei so unglaublich vielen granatenmäßig guten Ideen. Man fragt sich vorher, wieso gibt es denn das nicht schon längst? Das muss doch, das muss doch ein Thema sein. Weil wenn du sagst, natürlich haben alle, die im Netz irgendwie agieren, ein großes Interesse daran, dass die normale Infrastruktur um sie herum auch noch funktioniert. Digitalisierung ist für mich die schärfste Form der Ökonomisierung. Das heißt, Geld spielt dort eine überragende Rolle, sowohl bei der Entwicklung der, in Anführungsstrichen, guten Produkte oder Prozesse als auch eben bei den Katastrophengeschichten, die einfach nur dazu dienen, Dinge kaputt zu machen. Das heißt jetzt aufs Ehrenamt zu setzen und zu sagen: Mensch Meier, Freunde, wir wollen doch eigentlich alle, dass das hier... Das ist ja eine neue Dimension ist eigentlich was, was der Digitalisierung so überhaupt nicht entspricht, wo ja unglaublich vieles entweder passiert, völlig umsonst, also wenn ja, das wird dann einfach gemacht und wird dann in den Public Space da reingeschickt. Oder aber es geht ums Geld, es geht um richtig viel Geld dabei. Das heißt, das, was du da initiiert hast, ist ja schon Zivilgesellschaft, die wahrnimmt: Wir benutzen eine Infrastruktur, die müssen wir selber so gut schützen können, weil sie inzwischen in unserem Leben so eingedrungen ist wie eigentlich keine andere vorher. Also das ist schon was Besonderes.

Atug: *Na ja, kritische Infrastrukturen heißen ja nicht umsonst kritische Infrastrukturen. Sie sind ja kritisch für das Gemeinwohl und für das nachhaltige Altwerden. Ich sage immer: Auch morgen sollen meine Kinder noch kraftvoll in ein*

Glas Wasser schlürfen dürfen. Dazu müssen wir aber sicherstellen, dass morgen noch Frischwassergewinnung funktioniert, auch, wenn Sie digitalisiert wurde.

Lesch: Richtig.

Ich finde das Cyber Hilfswerk wirklich eine sensationelle Idee. Freiwillige Helferinnen und Helfer, die ausrücken, wenn gar nichts mehr geht. Manuel hat es eben so nett ausgedrückt. Was passiert, wenn aus Nullen Einsen werden? Digitale Systeme können nicht nur angegriffen werden, Software kann auch einfach veraltet sein. Systeme können ausfallen und dann geht plötzlich nichts mehr. Wie schlimm es wirklich werden kann, das wissen viele gar nicht. Denn die technische Unsicherheit ist sehr groß in Deutschland. Angriffe passieren viel häufiger, als wir annehmen. Prävention ist daher eine der Maßnahmen, die wir ergreifen können. Aber wir brauchen auch noch ein tieferes Verständnis davon, wie unsere komplexen Systeme wirklich zusammenspielen.

Atug: *Man sagt eigentlich, jeder wird irgendwann Ziel eines Angriffs. Die Frage ist nur, wann man zum Ziel wird und wann man es erkennt. Und darin liegt die Krux: Erkenne ich es früh genug, kann ich natürlich den Angriff komplett abwehren, erkenne ich es erst, nachdem der Angriff komplett durchgelaufen ist, dann stehe ich natürlich vor dem Trümmerhaufen. Das heißt, die Kunst ist nicht nur die Prävention zu machen, sondern in der Reaktion, im richtigen Moment möglichst früh oder viele, möglichst frühe Indikatoren zu haben, wo man drauf guckt und sagt: Könnte das was sein? Dann müssen wir jetzt schnell handeln. Und wenn das komplett ausbleibt, dann hat man natürlich keine Chance, dagegen zu agieren. Also ja, es geht. Aber man muss dafür bestimmte Basissicherheitsmaßnahmen*

täglich leben. Weil IT-Sicherheit oder Sicherheit generell ist halt kein Zustand, sondern es ist ein fortlaufender Prozess. Den muss sich aufrecht halten.

Lesch: Also man könnte schon davon sprechen, dass es sowas wie Achtsamkeitstraining geben muss, was die IT betrifft, dass man sich eigentlich möglichst empfindlich macht, dass man relativ früh feststellt: Ups, hier ist eine Performance-Veränderung. Aber das ist natürlich eine ganz neue Dimension für deutsche Verwaltung, sich auf einmal mit dieser virtuellen Welt zu beschäftigen, in der ja unglaublich viel, und das ist ja ein Punkt, wo ich mal einen winzigen Moment von diesen konkreten Fällen mal weggehen möchte, um mal so ganz allgemein über diese Digitalisierung zu sprechen. Das ist ja was völlig anderes als alles, was wir vorher an großen, sagen wir mal, ökonomischen und industriellen Veränderungen gehabt haben. Da hatten wir es ja immer mit Dingen zu tun, wir hatten es mit Sachen zu tun, die standen irgendwo, die waren dann entwickelt und man hat also über Innovationszyklen dann immer wieder gearbeitet dran, es ist besser gemacht, es ist optimiert worden. Bei der Digitalisierung geht alles viel schneller, es ist vielfältiger, also viel, viel, viel, viel mehr Varianten, weil es praktisch in sämtliche Lebensbereiche eindringt. Und da Anpassung an die Nutzung natürlich auch ständig sich vollzieht, auch da wieder der ökonomische Grundgedanke. Das ist, dass man sich ja tatsächlich die Frage stellen kann, ob wir überhaupt in der Lage sein werden, jemals als Zivilgesellschaft uns so achtsam werden zu lassen und so vorsichtig vielleicht auch damit umzugehen, dass wir uns wenigstens, soweit wir es irgendwie können, in den Zustand versetzen, nicht hysterisch zu werden oder Angst davor zu haben, dass irgendjemand uns den Strom abschaltet oder die Telekommunikation eines Tages weg ist. Und so weiter. Ich muss immer, vorhin, wo Du das sagtest, musste ich an Marc Elsbergs Buch denken, Blackout, wo das ja so richtig schön durchdekliniert wird. Und das war ja

offenbar auch für einige Energieversorger war dieser Roman ja ein Augenöffner und ich frage mich eben, das muss euch doch auch so passieren, dass es immer wieder Leute gibt, die sagen: Ach was, da habe ich noch nie daran gedacht, weil wir alle nicht dran denken. Das ist ja eine unglaubliche Herausforderung.

Atug: *Ja, also erlebe ich auf der Arbeit, beruflich natürlich sehr oft, dass die Leute nicht dran denken. Deswegen rufen sie uns ja und sagen: Könnt ihr mal draufgucken? Ihr habt viel mehr Erfahrungen habt eben ein breites Risikowissen oder auch Basissicherheitswissen und schaut ja strukturiert darauf, ob all diese Maßnahmen ineinandergreifen und funktionieren. Genauso bei der Prüfung, wenn man dann die Defizite aufdeckt. Aber als AG Kritis, das ganze Team schaut ja auch drauf und sieht auch immer wieder, dass wir mit Entscheiderinnen, mit Verbänden, Wirtschaftsverbänden und Lobbyisten reden oder eben auch mit den ganzen Politikerinnen etc., dass sie eben auch Digitalisierung nicht verstanden haben oder auch nicht kennen. Die haben halt mit IT nie zu tun gehabt. Teilweise sind das Denkstrukturen, ich bin jetzt mal ganz gehässig bei manchen Politiker*innen so in höchsten Ebenen, die sind auf dem Digitalisierungsniveau eines Faxgeräts. Und ich meine, das meine ich jetzt nicht böse. Die haben halt vor 50, 60 Jahren die Schule besucht und danach auch nie wieder mit diesem ganzen Digitalgedöns zu tun gehabt. Ich habe Politiker*innen erlebt, die etwas geringfügig älter als ich waren, aber wo dann gesagt wurde ja gleich kommt ein Büromitarbeiter und stellt dann die Websession her, damit wir dann auch sprechen können. Ich kann hier nichts anfassen und weiß auch nichts und darf auch nicht und so. Also digital inkompetent. So, und diese Inkompetenz rührt ja daraus, dass die gesamte Nation mehr oder weniger kaum strukturiert so was beigebracht bekommt.*

Genau aus dieser Technikunwissenheit, von der Manuel hier spricht, leitet sich dann ganz organisch auch die Idee für sein Cyber Hilfswerk ab. Denn, wenn diejenigen, die die Systeme bedienen nicht wissen, wie man sich richtig schützt, wie soll es dann überhaupt funktionieren, dass man große Hacking-Angriffe wie den auf Anhalt-Bitterfeld abwehren kann? Im letzten Teil unseres Gesprächs soll es deshalb darum gehen, wie man seine Idee eines Cyber Hilfswerks jetzt in die Tat umsetzt.

Lesch: So die Standardfrage wäre jetzt, gerade weil du ja mit dem CHW auch so eine großartige Idee hast, Menschen, die ehrenamtlich daran beteiligt sind, im Katastrophenfall zu helfen. Brauchen wir mehr Regulierung im Netz? Ist es eine Situation inzwischen, wo man grundsätzlich sagen müsste, also ganz unabhängig davon, ob es nun praktisch durchführbar ist oder nicht, müsste es nicht so was geben wie die Straßenverkehrsordnung? Wir haben die Datenschutzgrundverordnung in Deutschland, wo aber zum Beispiel auch ganz interessante Lücken drin sind. Sollte man das weiter verschärfen? Was ist da deine Meinung?

Atug: *Also meine Meinung wäre nicht verschärfen, sondern intelligent an Regulierung zu gehen.*

Lesch [00:50:23] Entschuldige meine Wortwahl, du hast völlig recht.

Atug: *Ja sorry, aber intelligent an Regulierung gehen bedeutet für mich, dass man sowohl natürlich Sanktionierung, aber auch Incentivierung betrachtet. Und ein Beispiel, es gibt ja jetzt das IT-Sicherheitsgesetz und IT-Sicherheitsgesetz zwei, da war ich ja dann auch im Bundestag als Sachverständiger und so, da haben wir*

eben auch gesehen, die ganze Kritik, die wir da abgeladen haben, um zu sagen, okay, das und das ist gut, aber kommen wir mal auf die Problemstellen, weil die sind ja wichtig und da haben alle sechs Sachverständigen wirklich sehr hart und sehr viel Kritik geliefert und auch durchaus Möglichkeiten und Lösungsansätze, wie man die angehen könnte. Die damalige Bundesregierung und das Innenministerium hat das alles entgegengenommen und gesagt: Ja, danke fürs Gespräch, wir lassen das Gesetz im Wesentlichen so und machen weiter. Gut kann man auch mit einer Wand reden, ist genauso effektiv. Also Kritikfähigkeit oder Selbstreflexion war da nicht so ausgeprägt. Viele Dinge, die jetzt im IT-Sicherheitsgesetz zwei stehen, sind eigentlich sogar kontraproduktiv für die Resilienz und Steigerung der Cybersicherheit in Deutschland oder auch die Widerstandsfähigkeit der kritischen Infrastrukturen. Diese Problemzonen geht man aber nicht an, weil teilweise die Lobby sehr stark ist, weil man sich irgendwie gedacht hat: Aber das ist doch dann die schlauere Variante. Oder man hat sich gar nichts dabei gedacht. Gibt es nämlich auch. Das heißt, ich würde mir wünschen, dass wir offener an diesem Diskurs und Dialog wirklich arbeiten und es nicht so ein Formakt ist, Leute einzuladen und dann sich das genervt anzuhören und anschließend doch so weiterzumachen, wie man will. Es ist schwierig. Diskurs ist immer schwieriger, als zu sagen: Ich gehe jetzt einfach links rum und dann ist gut. Aber der einfachste Weg ist nicht immer der richtige. Jetzt könnte man auch hingehen und sagen: Liebe Leute, wenn ihr eine kritische Infrastruktur seid und in Sicherheitsmaßnahmen, Basissicherheit, tägliche Sicherheit, Leben als Prozess etabliert, dann könnt ihr die Sachen einfach steuerlich absetzen. Wäre total bahnbrechend. Irre. Wahnsinn. Natürlich kostet das dann auch Geld. Aber der Benefit ist doch, dass morgen noch Strom und Wasser fließt. Das kann man gar nicht so blöd sein. Müsste man natürlich wieder überlegen: Wer kriegt aus welchen Gründen was für Gelder oder so? Aber man kann natürlich auch

Regulierung in eine Richtung treiben und sagen: Was sind denn die Ursprünge für die Auswirkungen, die wir erleben? Ein Ursprung ist schlechte Software. Es gibt keine sichere Software, es gibt immer Software mit Fehlern. Ja, Menschen machen Fehler und bei so und so viel Zeilen Programmcode ist immer einer drin. Aber es gibt ja durchaus im Stand der Wissenschaft sichere Systeme und man kann das bis zu einem gewissen Grad dahintreiben. Warum können, Stand heute, Airbag-Hersteller komplett dafür haften, wenn ein Airbag defekt ist und nicht sauber auslöst? Aber Softwarehersteller zucken mit den Achseln und sagen: Ja ist kaputt. Dann, vielleicht kriegst du einen Patch. Vielleicht kaufst du einfach die neue Version. Wir haben eine neue programmiert. Kostet nur wenige 10.000 Euro dann kannst du die auch noch haben. Warum geht das? Vielleicht brauchen wir ein Mindesthaltbarkeitsdatum für Software. Vielleicht brauchen wir auch Haftungsregulierung für Software. Wir müssen dann aber auch gucken, dass wir damit nicht Open Source zerstören, was ja auch ein sehr wichtiger Punkt ist, zu sagen habe ich eine kritische Infrastruktur, wo vor 30 Jahren was programmiert wurde, proprietär. Der Hersteller ist nicht mehr da, es gibt kein Update. Oder habe ich eine Open Source Software beauftragt und die in der kritischen Infrastruktur im Einsatz? Könnte also jederzeit jemand anderen rufen und sagen: Fuchs dich da rein und erweitere es mit neuen Sicherheitsmaßnahmen und Funktionalitäten. Muss man alles in einen Einklang kriegen und diskutieren und dann auch gute Regulierung machen und nicht schnelle Regulierung oder ignorante Regulierung.

Lesch: Gott sei Dank gibt es solche Menschen wie dich und deine Kolleginnen und Kollegen, die sich da zusammengetan haben mit der Wahnsinnsidee eine unabhängige Gruppe von Cybersecurity-Profis zu sein, die eben tatsächlich da in diesem Cyber Hilfswerk dann im entscheidenden Moment auch zur Seite stehen.

Und ich bin mir ganz sicher, wenn ihr zum Einsatz kommt, vor allen Dingen auch Hysterie verhindert und Panik verhindert. Um Gottes Willen, was ist?
Jetzt bleiben Sie mal ganz ruhig.

Atug: *Schnappatmung eingestellt. Alles wird gut, don't panic.*

Lesch: Genau stabile Seitenlage, Puls 60, kein Blutverlust und kein optischer Puls. Das ist immer ganz wichtig, dass da nichts passiert. Und das ist ja, das heißt, ihr habt ja schon Vorschläge gemacht, du hast ja schon Vorschläge gemacht. Und wenn es hinhaut mit dem CHW, wie sieht dann die Sicherheitswelt in Deutschland aus? Wird es dann mehrere Gruppen geben? Wie stellt ihr euch das vor?

Atug: *Also wie wir uns das vorstellen, haben wir ja in dem Konzept aufgeschrieben. Wie sich das am Ende umsetzt, wird natürlich maßgeblich auch davon abhängen, wo es aufgehangen wird und wie es umgesetzt wird und welche Behörden damit interagieren. Aktuell sieht es so aus, dass das Innenministerium offenbar plant, das ins THW zu integrieren, als eine weitere Funktionalität. Ich liebe das THW über alles. Es ist wirklich großartig, dass so eine Institution existiert mit über 85.000 Menschen, wovon mehr als 80.000 Ehrenamtlerinnen sind, die auch weltweit fast einmalig sind. Im Ausland im Einsatz sind und um wirklich den Leuten in katastrophalen Lagen so den blauen Hoffnungsschimmer bringen, weil sie die Blauen sind. Und trotzdem sind sie natürlich sehr konservativ, sehr schwergängig und tun sich mit IT sehr schwer. Das ist leider so, hat also auch ein paar Problemchen die, die man durchaus berücksichtigen muss. Aber sie haben auf der Habenseite und das ist sehr wichtig für uns und die Idee eines CHW, sie sind eben nicht-militärisch und sie werden auch nicht-militärisch eingesetzt. Das heißt, selbst wenn es in die Nähe einer militärischen Operation*

*käme, können die sagen: Machen wir nicht, wir sind nur für den Frieden da und tun diesen Dienst dann auch nicht. Und wir haben eben auch festgestellt, dass die Sicherheitsforscher*innen-Community in Deutschland und alle Hacker und Haecksen und auch die Menschen, die zum Beispiel jahrzehntelang in Leitständen von Kraftwerken oder so gearbeitet haben, die sich dann bei uns gemeldet haben und gesagt haben: Wann gibt es dieses CHW? Ich bin zwar in Rente, aber ich habe 40 Jahre in diesem Leitstand gesessen und die Dinger laufen noch 50 Jahre. Ich kann super Input geben. Das sind Menschen, die wollen was Gutes bewirken. Und wenn man denen eben das Signal gibt, dass es nicht eine rein gute Institution, die auch von der Gesetzgebung so instrumentalisiert wird, sondern vielleicht gibt die dann auch Informationen über diese Angriffsmethoden an Sicherheitsbehörden oder an das Militär weiter, dual use, kann man natürlich wieder zum Angriff gegen andere kritische Infrastrukturen einsetzen, dann wäre das eine Totgeburt. Und das haben wir natürlich ganz deutlich auch ins Konzept geschrieben und den Behörden mitgeteilt und gesagt: Leute, wenn ihr das macht, der Punkt Ethik und Moral ganz wichtig und die Gesetzgebung muss sein, denn die Community wird es nur machen on our terms, nach unseren Bedingungen. Und wir haben dazu ja nicht nur mit Institutionen wie dem BSI oder dem BBK, also Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Workshops gemacht, um dieses Konzept zu entwickeln. Wir haben ja auch mit dem CCC ganz offiziell zusammengesessen, sagt heute Workshop. Wir reden über die Bedingungen. Und die haben natürlich auch ausgearbeitet und gesagt: Klarer Fall. Wenn dieser Quatsch gemacht wird, dann werden wir sagen: Nee, so sind wir alle nicht dabei. Und wenn es so richtig mies läuft, dann werden wir sogar öffentlich kommunizieren: wer dabei ist, arbeitet für die falsche Seite, lasst es sein und dann ist das Ding tot. Und dann haben wir keine Ehrenamtler*innen da und das soll es natürlich auch nicht sein. Und deswegen versuchen wir diese Punkte natürlich*

auch hervorzuheben und zu betonen, dass hoffentlich das Innenministerium nicht in diese Richtung abdriftet oder die Lage so baut. Aber ja, wird man sehen, was kommt. Unser Angebot steht. Wir haben immer gesagt, wir stehen ehrenamtlich, beratend, begleitend zur Seite, wenn es eingeführt wird, als AG Kritis Team mit allen Mitgliederinnen und Mitgliedern. Und ja, wir warten auf den Anruf.

Lesch: Also wenn ihr jemanden braucht bei irgendeiner Anfangsveranstaltung für,was weiß ich,, ruf mich an, okay, ich bin dabei. Also ich finde das eine großartige, eine unheimlich tolle Idee. Ich danke dir sehr. Und ich weiß, das ist eine Idee, die kann die Welt wirklich richtig, besser, viel besser machen. Das ist eine tolle Idee Manuel. Also, ich bedanke mich auf jeden Fall bei Manuel Atug. Danke schön.

Atug: *Wunderbar.*

Lesch: Ja, wunderschön. Mann!

Ich gehe jetzt tatsächlich einigermaßen beruhigt aus diesem Gespräch. Vielleicht auch, weil ich weiß, wenn es hart auf hart kommt, dann gibt es Menschen wie Manuel Atug, die uns wahrscheinlich wieder aus dem Schlamassel rausholen können. Das war eine neue Folge Terra X, der Podcast. Vielen Dank fürs Zuhören. Diesen Podcast könnt ihr in der ZDF-Mediathek hören. Da gibt es auch die Skripte zu unseren Folgen und natürlich überall sonst, wo es Podcasts gibt. Und damit verabschiede ich mich im Namen des ganzen Terra X-Teams. Dieser Podcast ist eine Produktion von Kugel und Niere im Auftrag des ZDF.
Gute Nacht und viel Glück.