[Transcript] 11KM: der tagesschau-Podcast / Gehackt: Wie weiter nach der Cyberkatastrophe

Es ist der erste Cyber-Katastrophenfall Deutschlands, ausgelöst im Landkreis Anhalt-Bitterfeld.
Und da sieht es aus wie eine ganz normale Windows-Failer-Meldung.
In dem Fall stand da aber fett oben drüber, Landkreis Anhalt-Bitterfeld.
You are fucked. Do not touch anything.
Ein Hacker-Angriff legt die Kreisverwaltung praktisch komplett lahm.
Erst mal geht gar nichts mehr. Keine Sozialhilfeauszahlung, keine Autokennzeichen, keine Bescheinigungen.
Erst nach sieben Monaten erklärt Anhalt-Bitterfeld den Cyber-Katastrophenfall für beendet.
In dieser 11km-Folge erzählen wir, was wir aus diesem Hacker-Angriff von vor ziemlich genau zwei Jahren lernen können.
Vielleicht sogar müssen. Mit Marcel Roth vom MDR.
Denn solche Hacker-Angriffe werden immer häufiger. Marcel hat ausführlich zu dem Fall recherchiert
und mit ihm wollen wir rausfinden, was uns Deutschlands erste Cyber-Katastrophe über die kommunale IT-Sicherheit von heute verrät.
Ihr hört 11km der Tagesschau-Podcast, ein Thema in aller Tiefe.
Mein Name ist Victoria Michalsack. Heute ist Montag, der 10. Juli.
Marcel, herzlich willkommen. Hallo, danke, dass ich dabei sein darf.
Diese Geschichte spielt in Köten. Ich habe noch mal nachgesehen, wo das ist.
Das ist in der Nähe von Leipzig und Halle. Und zwar geht es los in einer Behörde.
In der Kreisverwaltung Anhalt-Bitterfeld. Marcel, sieht es da so aus, wie man sich das vorstellt?
Ja, so sieht es tatsächlich aus. Das ist ein Gebäude, ein altes Militärgebäude.
Dunkelblaue Teppichboden und links und rechts überall Türen.
Und unten so ein kleines Eingangshalle mit jemandem, der ein Viertner ist, hinter einer Scheibe.
Also ein ganz klassisches Behördengebäude, wo man jetzt nicht notwendigerweise besonders gerne hingeht.
Ja, so eine klassische Kreisverwaltung. Und da passiert was.
Am Dienstag, den 6. Juli 2021, den Mitarbeitern fällt da was auf.
Was passiert da?
Na ja, die kommen dann ganz normal hin. Stempelt sich ein.
Christian Wüstenberg zum Beispiel war eine, die in der Kfz-Stadt arbeitet.
Die schließt ihre Büro-Tür morgens auf, um halb sieben schon.
Also man startet da sehr früh im Sommer.
Bei Windows konnte ich mich noch ganz normal anmelden.
Bei unserer Fachanwendung war dann der Stopp da.
Das ging nicht mehr. Ich habe eine Fehlermeldung bekommen.
Also nicht schon wieder technische Probleme. Was soll das jetzt hier?
Ja gut, passiert manchmal, dass irgendwie die Technik nicht so richtig will.
Ist noch wem was aufgefallen?
Ja, dem IT-Menschen. Der sitzt auch zur gleichen Zeit, ein bisschen später.
Im Auto ist auf dem Weg nach Köthen, kriegt einen Anruf.
Olle, warum heißt der IT-Mensch?
Als ich dann auf der 183 war Richtung Köthen klingelt dann mein Telefon.

Der Kollege dann aus der Leitstelle dran, der dann sagte, hier ist irgendwas komisch.
Ich kann keine Datei mehr aufmachen. Hier ist alles doppelt da.
Die haben so eine ganz komische Endung.
Und die zweite Datei ist irgendwie immer so eine HTML-Endung.
Und da will er sich ein Tor brause installieren. Was ist denn da los?
Ich sage, ja, pass mal nix an. Ich bin gleich im Büro, ich gucke mir das an.
Olle, warum kommt dann auch sozusagen ins Büro, setzt sich an seinen Rechner
und stellt dann fest, das ist wirklich komisch.
Da sind nämlich alle Dateien doppelt.
Und es verdoppelt ist so ein Zeichen dafür, dass da so eine Datei verschlüsselt wurde.
Und dann kannst du die einfach nicht benutzen.
Dann kann sozusagen das Programm diese Datei nicht mehr lesen.
Man hat das nie trainiert, man hat keinen Handbuch in der Schublade
und sagt so jetzt das, das, das und das.
Sondern man handelt einfach intuitiv.
Erste Gedanke war, erstmal alles runterfahren, erstmal alles ausschalten,
dann kann erstmal nix mehr passieren, retten, was noch zu retten ist.
Dann hat die Olle Worms dann entschieden und mit dem Landrat gesprochen
und der Landrat sagt, naja, wenn wir es jetzt ausschalten wollen,
dann müssen wir das den Leuten ja mitteilen, weil E-Mail geht ja nicht.
Ja, ja klar.
Was bleibt da übrig? Okay, es bleibt da übrig.
A, eine Telefonkette, die gab es dann.
Und B, in Köthen gab es eine Lautsprecherdurchsage.
Ganz plump vom Viertner, der gesagt hat, bitte, liebe Kolleginnen und Kollegen,
schaltet eure Rechner sofort aus.
Okay, ist ja auch schon abgefahren.
Noch mal zum Verständnis.
Wir sind eigentlich in Köthen, aber wir sind auch gleichzeitig noch
an ganz vielen anderen Standorten.
Also da hängt viel mehr dran und alle können sozusagen plötzlich
an dem 6. Juli 2021 nicht mehr an ihre Daten.
Und ein paar Tage später macht dann so ein Screenshot eine Runde,
ein Screenshot, den jemand angefertigt hat von einem Server
und da sieht es aus wie eine ganz normale Windows-Fehlermeldung.
Und in dem Fall stand da aber fett oben drüber, Landkreis, Anhalt, Bitterfeld,
you are fucked.
You not touch anything.
Und dann stand irgendwie hier ein Passwort, eine ganz lange kryptische Internetadresse.
Das ist ja eine Hausche, Ansprache, das ist ja eine Message.
Das ist die erste Message von Hecker, die dir damit den Mittelfing einfach zeigen.
Die dir damit zeigen, ja, du hast dir nicht nur irgendwas Komisches eingefangen,
sondern du wurdest gehackt.

Du wurdest gehackt, genau.
Können die denn zu dem Moment eigentlich einschätzen,
was das jetzt für die bedeutet?
Nee, ich glaube in dem Moment nicht.
Ich glaube, der Groschen gefallen ist am Donnerstag-Vormittag tatsächlich.
Wo wirklich die ganze Band breitet, die ganze Dramatik sich entfaltet hat.
Auslöser dafür war ein Telefonat.
Es gab nämlich so im Land auch Telefonate, das dem mal gesagt hat,
wir haben hier einen IT-Experten, Thomas Leich heißt der,
der ist Professor an der Hochschule Harz, hat mit IT zu tun.
War IT-Berater, hat auch sozusagen in solchen Fällen schon mal Firmen beraten,
hat über solche Fälle auch schon mal Firmen Pleite gehen sehen.
Der kriegt einen Anruf aus, sagt es an als Digital-Masterium.
Thomas, kannst du mal bitte den Oliver Rumpf in Köthen anrufen.
Der hat da so ein Problem, redet doch mal miteinander.
Und während die telefonieren, also der Oliver Rumpf und der Thomas Leich
und während die miteinander gesprochen haben über den Virus,
und das alles irgendwie ganz komisch ist,
sitzt sozusagen der Kollege von Oliver Rumpf gegenüber
und sieht, wie sich der Rechner verschlüsselt,
wie sich sein eigener Rechner verschlüsselt,
was eigentlich bisher nicht so klar war, dass das funktioniert,
weil dieser Rechner eigentlich nur sozusagen per Fernwartung
auf den Server geguckt hat.
Und das zeigt eigentlich, dass diese Schadsoftware
wirklich verschiedene Netze gleichzeitig angreift
oder von Netz zu Netz gehen kann.
Das erzählt ich halt an Leicht direkt am Telefon.
Und dann sagt er, das ist richtig gefährlich,
Notruf ans Land absetzen.
Das hier ist Cyberterrorismus, das könnt ihr nicht alleine bewältigen.
Und das ist so der Auslöser, wo Thomas Leich sagt,
ihr habt da richtig, richtig die Scheiße am Hacken.
Der sagt sogar, das ist sowas wie Cyberterrorismus.
Also informiert den Landrat, das ist richtig heftig, was ihr da habt,
der hat da so ein Bild gemalt, hat gesagt, was ist,
stellt euch vor oder sagt dem Landrat,
der ist auch schon ein bisschen was älter als Landrat,
sagt dem Landrat, der soll dich vorstellen, den Bitterfett,
steht jetzt die Elbe zwei Meter hoch in den Straßen.
So eine Situation habt ihr jetzt altimäßig.
Das hat er denen gesagt.
Also der hat gesagt, Leute, das hier, das ist ein richtiger Notfall,

der spricht von Terrorismus.
Und deswegen wird auch Katastrophenalarm ausgelöst.
Und das gab es tatsächlich noch nie,
dass ein Katastrophenalarm ausgerufen wurde
wegen einem IT-Notfall, wegen einem Cyberangriff.
Richtig.
Wenn du den Katastrophenfall ausrufst,
kannst du eben auch bestimmte Sachen als Landrat einfach bestimmen.
Kannst du einfach sagen, wir kaufen jetzt mal hier ein paar neue Rechner
oder wir beauftragen jetzt mal diese Firma XY.
Oder wir beantragen jetzt mal Hilfe bei anderen Behörden.
Und die Behörden können das da nicht so einfach ablehnen.
Also so ein Katastrophenfall ausrufen,
da gehört schon Mut dazu in so einer Situation,
weil du sagst, weil du dich ja völlig nackig machst,
du sagst ja wirklich vor aller Welt,
wir stehen ja mit dem Landrat,
wir können uns nicht helfen, bitte helft uns.
Das kleine IT-Team vor Ort ist also überfordert,
hofft auf Hilfe.
Und die Kreisverwaltung bleibt erst mal komplett lahmgelegt.
Die Polizei ermittelt auch schon gegen die Hacker.
Vier Tage ist der Angriff jetzt her.
Marcel, diese Hacker, die haben ja diese kryptischen Internet-Adressen
auf den Computern hinterlassen.
Was ist denn eigentlich passiert, wenn man da draufgeklickt hat?
Wenn du da draufgegangen bist, dann stand da eben,
jawoll, wir haben dich, Landkreis Anhalt Bitterfett,
you have been hacked.
Diese Seite, die du gerade siehst
und der Entschlüsselungskode,
der läuft in 21 Tagen aus.
Bitte zahl doch 500.000 Dollar, eine halbe Million Euro.
Ansonsten veröffentlicht wär deine Daten.
Nein.
Und die schreiben auch, im Normalfall kostet so ein,
der Wiederaufbau von gehacktem System,
kostet durchschnittlich 3,5 Millionen Euro.
Schreiben die auch auf ihrer Seite.
5.000 Euro aus deren Sicht.
Irgendwie natürlich ein Schnäppchen.
Die Info liefern Sie auch noch mit, dass es sich lohnen würde.
Ja, genau.

Wahnsinn.
Sie ist Erpressungsgeld.
Da hat man relativ schnell gesagt, kurz überlegt,
nee, zahlen wir nicht, die öffentliche Hand zahlt,
lässt sich nicht erpressen.
Ich wüsste auch gar nicht, wie so ein Kamera so was verbucht,
ehrlich gesagt.
Als Sonderausgabe.
Okay, wir haben also eine quasi komplett lahmgelegte Verwaltung.
Die Polizei ermittelt zwar,
aber klar ist auch, an die Erpresser soll kein Geld gezahlt werden.
Aber es ist ja alles lahmgelegt.
Wer hilft denn jetzt dem IT-Team?
Also es kommt tatsächlich jemand vom BSI,
vom Bundesamt für Sicherheit in der Informationstechnik,
schon direkt an dem Tag,
als der Katastrophenwalarm ausgerufen wurde,
kommt jemand nach Köthen und entscheidet,
oh, ich bleib mal übers Wochenende
und bring euch mal so ein bisschen auf die Fahrt.
Zweites Schritt war dann zu sagen, okay,
wir müssen jetzt ein Notnetz aufbauen,
dass wir irgendwie digital wieder untereinander kommunizieren können.
Und parallel fängst du an zu überlegen,
wie sieht denn jetzt eigentlich meine IT-Infrastruktur neu gemacht aus?
Was muss ich denn da wie aufbauen und wie auch verstecken
und wie muss ich vielleicht meine Server nochmal neu konfigurieren?
Und also was.
Und währenddessen musst du noch überlegen,
sind die Täter eigentlich so dick in dem System drin,
dass die vielleicht, wenn wir wieder neu starten, immer noch drin sind?
Also das sind alle so Fragen, die da irgendwie beantworten werden müssen.
Und du merkst, dass die Riesenratten schon ins Nachsicht,
das ist Riesenarbeit.
Wir müssen immer klar machen,
das ist ein Langlauf und kein Sprint.
Und das nächste ist natürlich dann mit den verantwortlichen Pläne
für die Zukunft aufzuarbeiten halt.
Also sich auch wirklich mal Gedanken zu machen
und nicht die ganzen Schnellschüsse, die eigentlich üblich sind,
weil man möchte eigentlich, man erwartet so ein bisschen nächste Woche,
kann die IT wieder weiterlaufen.
Aber die Realität sieht halt da ganz anders aus.

Ich habe mir im Podcast auch mit Dirk Herr gesprochen,
der ist sozusagen der Chef dieser schnellen,
na ja ich nennt mal, Cyber-Eingreif-Truppe beim BSI.
Wir sind auch dafür da, Opfern eine stabile Seitenlage zu bringen.
Wir haben die Ersthilfe.
Aber wir müssen uns einfach relativ schnell rausziehen.
Es darf nicht der Normalfall sein, dass wir vor Ort aufräumen.
Das müssen die Opfer eines Angriffs schon selber tun.
Also BSI-Menschen sind da, die sozusagen Ahnung haben
und die sich das einen Wochenende lang angucken und sagen,
ja, jetzt seid ihr auf der Spur.
Und dann am Sonntag alle schick, wir fahren wir zurück,
ihr seid in der stabilen Seitenlage.
Danke.
Und dann war relativ schnell klar, wir brauchen Hilfe.
Wir holen uns eine IT-Forensikfirma.
Das sind so Menschen, die wirklich genau wissen,
okay, wie haben sich die Täter bewegt in unserem Netz?
Welche Sicherheitsvorkehrungen haben wir eigentlich gehabt?
Und die entscheidende Frage aber, kommen wir an die Backamps?
Können wir mit den Daten irgendwas anfangen?
Die verschüttelt sind, können wir die vielleicht entschlüsseln?
Also das sind also Fragen, die IT-Forensiker beackern können.
Für diese Firma war klar, okay, da muss ja irgendwie Geld da sein.
Muss irgendwie mal bezahlen.
Das sind Leute, die ganz schnell im Einsatz sind, die hochqualifiziert sind,
die auch hochqualifiziert bezahlt werden sozusagen.
Und da gab es eine Zusage von der Landesregierung von Sachsen-Anhalt.
Pass mal auf, IT-Forensik würden wie erst mal übernehmen,
eine Viertelmillion Euro, Pima, Daumen,
würden wir euch da zur Verfügung stellen.
So, dann ist man als Landtag, glaube ich, einmal sehr entspannt.
Führte tatsächlich aber dazu, Victoria,
dass das Geld nach neun Tagen alle war.
Nach neun Tagen klingt jetzt angesichts dessen,
dass wir schon gesagt haben, dass es ne Riesenkatastrophe ist.
Echt nicht so lang.
Nee, das war sozusagen von einem Montag bis zum darauffolgenden Dienstag,
inklusive Wochenende sozusagen.
Da gab es ein Gespräch beim Landrat,
und da hat man festgestellt, Hoppala, 245.000 Euro sind schon weg.
Mehr Geld haben wir nicht.
Und dann sagt ne Firma, was sagt die wohl?

Ja, dann?
Sind wir weg, wiedersehen, danke.
Oh je.
Und das heißt, die Experten waren wieder weg
und die waren immer noch gehackt
und hatten das ganze Geld verbraucht, oder wie?
Genauso.
Allerdings kam dann, und das ist tatsächlich ungewöhnlich,
das BSI wieder mit ein paar mehr Leuten
und hat dem Landkreis daran geholfen.
BSI klingt immer also schön, klingt auch schön in Pressemittragung.
Das BSI ist da, wir kriegen Unterstützung vom BSI.
Aber ganz ehrlich, die sind nicht zuständig.
Wie die sind nicht zuständig?
Ich dachte, die sind für Hacker Angriffe zuständig.
Bei kritischer Infrastruktur, Energieversorgung
und eben auch bei Bundesbehörden, bei Bundesverwaltungen.
Hier reden wir über eine Kreisverwaltung.
Ach.
Naja, Tata, für der Rallismus.
Naja, aber also da denke ich mir…
XA, aber das ist nicht zuständig.
Ja gut, aber die arme Kreisverwaltung.
Also die haben eigentlich aus Nettigkeit nur gereifen.
Ja, und auch, weil man gedacht hat, diese Schadsoftware
könnte auch für Bundesbehörden schwierig werden.
Das Projekt IT Wiederaufbau fängt also an
mit einem krassen Kompetenzbürer
und mit akutem Expertenmangel.
Ich gehe jetzt noch mal einen Schritt zurück,
weil ich mich frage, abgesehen davon,
dass die Leute ihre Büroarbeit nicht machen können.
Was bedeutet das denn für die Bürgerinnen und Bürger,
für die die Kreisverwaltung ja da ist,
für die ich glaube, es sind über 150.000 Einwohner da im Landkreis.
Was heißt das für die, wenn da nichts mehr geht?
So ein Landkreis hat zum einen natürlich auch die Aufgabe,
Sozialleistungen auszuschütten.
Für Wohngeld zum Beispiel.
Oder für Menschen mit Behinderung.
Dann hat der Landkreis Aufgaben zum Beispiel die Autokennzeichen
auszustellen, müssen ausgestellt werden.
Oder der Landkreis hat zum Beispiel eine Ausländerbehörde.

Da geht es sozusagen um Menschen, die aus dem Ausland kommen
und die an welche Papiere brauchen.
Also da kommt ganz viel zustande.
Kurz sozusagen die Sozialleistung,
das wurde relativ unbürokratisch dann gelöst,
weil das unmittelbar entscheidend auch ist,
dass sie sich sozusagen hungern müssen.
Das ist ganz entscheidend.
Und das haben die dann einfach so gelöst,
die haben mit ihren Banken gesprochen, haben gesagt,
liebe Banken, überweist doch bitte einfach das Geld,
was ihr Anfang Juli überwiesen habt, im August nochmal.
Die zweite Sache mit den Autokennzeichen,
das ging tatsächlich dann über Wochen überhaupt nicht.
Also, das heißt, jetzt ist da bei denen Ausnahmezustand.
Abgebrannt.
Ja, wie läuft das denn jetzt bei denen weiter?
Da kann man sich das vorstellen, was passiert in dieser Behörde?
Was Oliver Rumpf macht sozusagen ist,
die haben sich gegenüber vom Landratsbüro,
haben sich so ein Besprechungsraum genommen,
da sitzen die drin, musst du dir vorstellen,
da sitzen so sagen jetzt die Leute vom BSI drin,
da sitzt die technische Einsatzleitung drin,
da sitzen die zwei, der Oliver Rumpf und der zweite Kollege,
der noch an die Infrastruktur macht, drin.
Wir haben es war rum genannt, hier haben wir unseren Krieg geführt.
Ja, in dem Büro hat eigentlich alles stattgefunden.
Wir haben ja gelebt.
Wir arbeiten aus, arbeiten die und entwickeln halt so Sachen.
Oder stellen zum Beispiel dann auch mal Amtshilfeanträge,
zum Beispiel auch ein Amtshilfeantrag an die Bundeswehr.
Und wer kommt dann da?
Kommt dann da Soldaten in Flecktarn?
Wer kommt denn da?
Soll ich dir was sagen?
Diese Frage habe ich auch gestellt
und dann hatte ich so den Gefühl,
die Antwort bei den Soldaten, was ist denn eine dumme Frage?
Ja, Soldaten in Uniformen kommen bei der Bundeswehr,
überradenderweise.
Aber dann bin ich beruhigt,
dass du die dumme Frage ausgestellt hast.

Genau, genau, genau.
Das sind Soldaten vom Kommando ZIR,
Cyber- und Informationsraum.
Die haben insgesamt 14.000 Soldaten über ganz Deutschland verteilt.
Sind sozusagen eigentlich für die IT der Bundeswehr zuständig
und kennen sich natürlich entsprechend auch mit Cyber-Sicherheit aus.
Und die kamen halt nach Annalpitterfeld und haben da geholfen.
Haben geholfen, IT-Sicherheitskonzept zu schreiben.
Wie macht man seine Systeme sicher?
Also für den Wiederaufbau was ganz Wichtiges.
Haben aber eben auch ganz profan die Computer genommen,
die da waren, unter Anleitung von Oliver Rumpf,
haben sich die angeschaut
und haben da neue Betriebssysteme drauf gespielt.
Also haben die platt gemacht und neu bespielt.
Ganz plump, jetzt mal so gesagt.
Und mit deren Hilfe lief das Ganze dann wenigstens so ein bisschen?
Richtig.
Aber wenn ich es richtig gelesen habe,
dann hat es ja ganze sieben Monate gedauert,
bis der Landkreis diesen Statuskatastrophenfall wieder aufgehoben hat.
Und da war ja immer noch nicht alles wieder hergestellt.
Und was die Hacker dann mit den Daten machen oder noch machen werden,
weiß keiner.
Plus, es war ein Riesenaufwand.
Wie viel hat das jetzt eigentlich am Ende gekostet,
dieser Wiederaufbau.
Die Hacker haben ja behauptet, das wird unglaublich viel.
Und deswegen soll man Losegeld zahlen.
Wie viel hat es am Ende wirklich gekostet?
Also der Landrat hat mir letzten noch gesagt,
2,5 Millionen Euro hat das alles gekostet.
Dazu die 250.000, die sozusagen das Land übernommen hat.
Wenn man jetzt ehrlich ist, müsste man rechnen,
was hat eigentlich das BSI gekostet?
Das haben eigentlich die Bundeswehrleute gekostet.
Die stecken in der Rechnung nicht mit drin.
Ich halte 3,5 Millionen nicht für aus der Luft gegriffen,
was die Hacker sozusagen da am Anfang behauptet haben.
Was weiß man denn eigentlich über diese Hacker oder Hackerinnen da?
Wer war es denn?
Das war eine Crime-Geschichte.
So, was machst du, Hacker?

Pay or Grief, so haben die sich genannt.
Ich bin als erstes natürlich zu unserem Landeskriminalamt gegangen.
Die sagten, ja, Pay or Grief.
Wo die herkommen, wissen wir nicht.
Wir haben Amtshilfeersuchen in verschiedene Länder gestellt,
dass die uns da unterstützen.
Was halt so eine Polizei sagt, wenn sie noch im Ermittlungsverfahren ist.
Ich bin rausgegangen mit dem Gefühl, naja.
Danke, die kriegen die sowieso nicht.
Und dann gab es Anfang März 2023
eine Pressekonferenz in Düsseldorf beim LKA Nordrhein-Westfalen.
Und dann schrieb mir mein Chef eine Nachricht,
man seh, guck mal, die haben die Täter ermittelt.
Da war ich wirklich am Tippen und noch sozusagen am Schneiden
von dem ganzen Material.
Da kam die Nachricht und ich dachte, was?
Wie? Die haben die Täter ermittelt. Wer denn bitte?
Und dann eben diese Pressekonferenz im März, wo das LKA Nordrhein-Westfalen sagt,
wir wissen, wer die Uniklinik Düsseldorf gehackt hat.
Wir wissen, wer die Funke Mediengruppe gehackt hat.
Wir wissen, wer Matratzenkonkord gehackt hat.
Und das ist die selbe Gruppe, die Anhalt Bitterfeld gehackt hat.
Wir reden in Deutschland über 37 Fälle, weltweit über mehr als 600 Fälle.
Und dann hast du eben da drei Russen, die mit internationalem Haftbefehl
gesucht werden, auf Europe's Most Wanted Liste stehen
und die, von denen es freundliche Fotos aus sozialen Netzwerken gibt.
Und die in Russland leben.
Diese Hackergruppe ist übrigens ein ganz eigener Fall für sich,
wenn ihr mehr über die wissen wollt.
In Marcel's Podcast rein, you are fucked.
Deutschlands erste Cyberkatastrophe.
Link bekommt ihr in den Shownotes.
An diesem internationalen Haftbefehl sieht man ja auf jeden Fall,
dass man das ernst nehmen sollte.
Und diese Hackergruppe soll auch nicht nur verantwortlich sein
für den Cyberangriff auf diese Behörde in Anhalt Bitterfeld,
es geht auch noch um einige andere.
Und weil du gerade das Universitätsklinikum Düsseldorf erwähnt hast,
da musste wohl, weil nämlich die Klinik gehackt wurde,
ein Krankenwagen abgewiesen werden mit einer Person in Lebensgefahr.
Und ich finde, das macht nochmal ganz deutlich,
warum wir hier darüber reden.
Weil das nämlich echt gefährlich werden kann und echt Kreise zieht.

Total, total.
Also ich frage mich, wenn das so gravierend ist.
Und gleichzeitig hören wir das Bundesbehörden,
wie das BSI eigentlich gar nicht zuständig sind.
Wie kann das denn sein?
Da kann ich hier mit einem Wort darauf antworten.
Föderalismus.
Es ist tatsächlich so,
dass in Deutschland die 11.000 Kommunen,
die 400 Landkreise,
die sind für ihre IT-Sicherheit selbst zuständig.
Das ist ein bisschen, ich finde es auch unbefriedigend, ehrlich gesagt.
Das lässt mich auch in der Recherche so ein bisschen ratlos zurück.
Der Thomas Leicht, der Professor vor der Hochschule Haarten,
von dem wir anfang erzählt haben, der der erste war,
der da ein bisschen geholfen hat.
Mit ihm habe ich zusammengesessen, der hat mir das erzählt
und sagt, hey, weißte, weißte.
Also ein IT-Service im Landkreis ist ja Infrastruktur.
Da sitzen wir hier in Magdeburg.
Ich könnte ja auch jemanden sein, der die Elbbrücke mal wegbompt.
Und sage übrigens, du hast noch zwei weitere Elbbrücken,
zahl mal die Summe X.
Es ist ja nichts anderes,
als die im Prinzip mit diesem Trojaner machen.
Deswegen verlangst du aber nicht von der Oberbürgermeisterin hier,
dass die irgendwelche Abwehrraketen um diese Brücke stellt.
Das ist ganz klar geregelt.
Diese Brücke wird für Luft angriffen,
von der Bundesrepublik Deutschland ausgeschützt.
Obwohl es eine kommunale Brücke ist,
muss ich da die Oberbürgermeisterin nicht darüber Gedanken machen,
dass hier jemand international vorbeifliegen kann
und kann da mal was drauf werfen.
IT-technisch ist das so.
Man muss den Bild gar nicht zustimmen,
aber das hat mir so ein bisschen klargemacht, stimmt irgendwie.
Das ist komisch.
Also offensichtlich sind wir noch nicht darauf vorbereitet,
wie auf andere Katastrophen.
Die Kreisverwaltung in Anhalt-Bitterfeld war es offenbar nicht.
Jetzt frage ich mich, jetzt ist das so passiert.
Haben die Verwaltung in Deutschland

aus dieser ersten Cyberkatastrophe was gelernt?
Und wenn ja was?
Ich habe schon gesagt, 11.000 Gemeinden, 400 Landkreise.
Also das ist eine Frage, die uns auch wirklich umgetrieben hat.
Ich kann mir die selbst auch gar nicht zufriedenstellend beantworten.
Ich glaube aber tatsächlich dieser Fall,
der ist herausragend, weil Katastrophen fahren,
der ging total durch die Presse.
Ich glaube schon, dass der bei vielen IT-Verantwortung
nicht was ausgelöst hat.
Und auch bei vielen entscheidungsträgern,
also politischen entscheidungsträgern, Bürgermeistern und so was.
Dass dem klar wurde, Hopper lagen, kann uns das auch passieren?
Allein sich diese Frage zu stellen,
ist schon Teil der Lösung, finde ich.
Also mein Gefühl ist, da kommt ganz viel jetzt ins Rollen.
Ich habe mit jemandem aus dem Bundesministerium gesprochen
und habe auch gefragt, wie würden sie sich denn einschätzen?
Wie sind denn die Kommunen so aufgestellt?
Und der sagte mir, naja, so Pi mal Daumen, ein Drittel,
kein Problem, alles super, die kriegen das gewuppt.
Das andere Drittel, ja, die kriegen das schon hin,
die haben sich auf den Weg gemacht.
Und das dritte Drittel, die haben keine Ahnung.
Also es gibt keine Statistik darüber,
wie gut sind die Kommunen und Landkreise in Deutschland
eigentlich IT-mäßig aufgestellt.
Ich weiß auch nicht, ob der Katastrophenfall,
ob es so simpel ist, zu sagen, Katastrophenfall auslösen,
reicht und wir kriegen Hilfe.
Man muss halt vorbereitet sein.
Ja, also das heißt aber, niemand weiß,
wie es wirklich um die IT-Sicherheit in Deutschland steht.
Nee.
Das ist ja wirklich ein bisschen verrückt, oder?
Also, ja, um die IT-Sicherheit von Kommunen und Landkreisen,
das ist ein bisschen verrückt, ja.
Kann nur gezählt werden, soviel Fälle hatten wir.
Was wir in der Recherche aber auch ausgefunden haben
und das war so ein bisschen ein Erlebnis für mich,
es gibt ein nationales Cyber-Abwehrzentrum.
Da sitzen zehn Organisationen drin,
unter anderem das BKA von der Bundeswehrleute,

das BSI natürlich, also wirklich verschiedene Organisationen.
Und dieses nationales Cyber-Abwehrzentrum hat sich
Anfang des Jahres mal damit beschäftigt,
wie sieht es denn eigentlich in der IT-Sicherheit in Kommunen aus?
Das war deren Fragestellung, die hatten so eine Arbeitsgruppe,
haben dazu auch ein Papier geschrieben.
Ich habe eine Anfrage an das Bundesinnenministerium dazu geschrieben,
gibt es dieses Papier?
Ja, gibt es, könnt ihr dazu mal sagen, was da drin steht?
Nee, können wir leider nicht sagen, weil Verschlusssache.
Okay, kann man verstehen.
Was mich aber dann, also tatsächlich total fuchst,
ist die Antwort auf meine letzte Frage an die.
Die letzte Frage, die ich die Gestellte habe war nämlich,
können denn wenigstens die Kommunen da reingucken?
Wissen die denn, was ihr da herausgefunden habt
oder was ihr meint, was wichtig ist?
Und da war die Antwort, nein.
Das ist eine Bundestache und da gucken die Kommunen nicht rein.
Also das ist Verschlusssache, da dürft ihr nichts von wissen.
Nee, nicht wegen der Verschlusssache, sondern weil
das nicht die Zuständigkeit des Bundes ist.
Der Bund hat keine Zuständigkeit für Kommunen.
Da sind wir nicht zuständig.
Ja, gut, dann nicht.
Also es ist einfach ein aktuelles Problem.
Es gibt immer wieder solche halbe Angriffe.
Das wird immer normaler auf eine traurige Art und Weise.
Und man hat aber nicht das Gefühl,
dass es dafür eine Vorbereitung gibt, wie für andere Sachen.
Wie zum Beispiel einen Brand in einem Gebäude oder so.
Das ist nicht so ein Notfallplan, ne?
Und keine Übungen, es gibt keinen Notfallplan, genau.
Wo du sagst, wie wir am Anfang hatten, Schublade auf.
Ich muss jetzt das und das und das machen.
Denen kann ich anrufen.
Und meine Organisation stelle ich jetzt so um.
Ja, das gibt es irgendwie noch nicht.
Meinst du, das gibt es in den nächsten Jahren?
Ja.
Okay, also du bist guter Dinge, das freut mich.
Wie geht es denn jetzt eigentlich der Kreisverwaltung
an Halb-Bitterfeld heute?

Also der Landkreis sagt heute,
sie sind zu 98 Prozent wieder da, wo sie vorher waren
und 90 Prozent der Daten seien wieder hergestellt.
Das ist doch eine ganz gute Zahl, oder?
Also es ist zumindest was, wo man sagt,
ja, Wolls funktioniert wieder einigermaßen, genau.
Kann man mit zufrieden sein, ob das jetzt zwei Jahre lang dauern muss.
Das ist natürlich irgendwie zu hoffen,
dass das demnächst nicht mehr so lange dauert.
Okay.
Marcel, vielen Dank, dass du uns davon erzählt hast.
Ich habe viel gelernt.
Sehr gern.
Und nochmal reinschalten, ne?
Genau.
Noch tiefer in diesem Fall eintauchen,
könnt ihr in Marcel's Podcast-Reihe
You Are Fakt Deutschlands erste Cyberkatastrophe.
Ihr findet sie in der AID-Audiothek
und auch überall sonst host Podcasts gibt, genau wie uns.
Das war Elfkm für heute.
Autorin dieser Folge ist Marlene Obst.
Mitgearbeitet hat Stefan Beutting.
Produktion Fabian Zweck, Florian Teichmann,
Hannah Brünjes und Christopher Newerf.
Redaktionsleitung Lena Gürtler und Fumiko Lipp.
Elfkm ist eine Produktion von BR24 und NDR Info.
Mein Name ist Victoria Michalsack.
Wir hören uns morgen wieder.
Tschüss.