Ich bin Schold Wilhelm, das ist Thema des Tages, der Nachrichten-Podcast vom Standard.
Da kommt eine Nachricht und da sagt eine Person, ich habe hier Material über eine Firma, hinter der sich russische Geheimdienste verstecken.
Eine geheime Firma, die Putin-Cyber-Krieg ermöglicht.
Eine Firma, die Waffen zur Überwachung, Desinformation und Angriffe auf kritische Infrastruktur entwickelt.
Sie sehen mittlerweile fünf Bereiche, wo sie Krieg führen.
Und zwar ist es auf dem Wasser, in der Luft, auf dem Land, im Weltall und im Fünften des Standard-Cyberspace,
im Internet, wo wir alle zum Ziel werden können.
Enttarnt von einem Whistleblower und einem Netzwerk internationaler Medien.
Heute sprechen wir über die Vulkan-Files.
Darüber, die Russland-Cyber-Krieger, die Ukraine lahmlegen.
Man sozusagen live zuschauen musste, wie Fremde die Kontrolle übernommen haben und dafür gesorgt haben, dass in Krankenhäusern, Kindergärten und so weiter der Strom ausgefallen ist.
Wir sprechen darüber, wie Putin's Hacker längst auch kritische Ziele in Deutschland, Österreich und ganz Europa attackieren.
Und ob wir langfristig mit einem folgenreichen Schlagabtausch zwischen Russland und dem Westen rechnen müssen.
Hannes Munzinger, du bist investigativ, Journalist und von Beginn an in die Recherche involviert.
Wie und wo fängt denn diese Geschichte an?
Die Geschichte fängt vor ungefähr einem Jahr an.
Es sind erst wenige Tage seit Beginn des Kriegsen der Ukraine vergangen.
Da kommt eine Nachricht in einem sicheren Postfach an, die ich lese.
Ich bin damals noch Journalist bei der Süddeutschen Zeitung und da sagt eine Person, ich habe hier Material über eine Firma hinter der sich russische Geheimdienste verstecken.
Wollt ihr euch das mal anschauen?
Wer ist denn diese ominöse Person, die sich aus ihm nichts meldet?
Wer ist dieser Whistleblower und warum hat das sich an dich oder an euch gewandt?
Wir können sehr wenig über diese Person sagen.
Einerseits natürlich aus Quellenschutzgründen, andererseits weil wir es größtenteils auch nicht wissen,
weil es eben der Kontakt zunächst über so ein anonymes System entstanden ist,
das extra dazu da ist, dass Leute sich melden können, ohne dass ihre Identität offengelegt werden muss.
Deswegen wissen wir nur etwas über die Motivation dieser Person, die eben sagte,
mich regt auf, was da in der Ukraine passiert, ich will das nicht so hinnehmen, ich will was tun.
Und die dann eben sagte, ich habe diese Information mit dieser Firma und dahinter verstecken sich Geheimdienste,
das ist eine Tarnoperation und die Leute sollen die Gefahren kennen können, die dahinter stecken.
Aber du hast diese Person tatsächlich nicht selbst getroffen?
Nein, leider nicht.
Diese Person meldet sich bei euch, dieser Whistleblower und sagt, er hat da etwas, er weiß etwas,

er weiß es, unzufrieden mit der Situation in der Ukraine, er weiß, dass da mehr dahinter steckt und er meldet sich mit Dokumenten, mit Unterlagen.
Wie muss man sich diese Dokumente vorstellen, woher stammen die, was beschreiben die?
Also was wir haben, sind mehr als 1000 Dateien, die ganz offensichtlich aus dem Inneren einer russischen Firma stammen.
Diese Firma heißt Vulkan, deswegen nennen wir die Recherche auch Vulkanpfeils und das ist eine Zulieferfirma
im Prinzip für die Geheimdienste, die Software entwickelt.
Und was die Quelle uns übergeben hat, sind im Wesentlichen sehr viele Dokumente, die Softwareprojekte beschreiben,
also Programmbeschreibungen, Anleitungen für Nutzeranleitungen für Administratoren, Testabläufe, Konzepte,
unterschiedlichste Dokumente, alle auf Russisch, dazu sehr viele Firmen, interne E-Mails, Excel-Sheets, alles Mögliche.
Wofür soll denn Russland diese Firma Vulkan ganz konkret eingesetzt haben?
Was geht denn aus diesen Dokumenten hervor?
Also aus den Dokumenten geht hervor, dass die drei wichtigsten Geheimdienste,
das Verteidigungsministerium und das Militär mit dieser Firma zusammenarbeiten und diese Firma Software
gebaut hat, entwickelt hat, die mit Desinformationen zusammenhängt, die bestimmte Zensur leisten kann,
die möglicherweise auch Überwachung leisten kann, zum Beispiel von sozialen Netzwerken, um Proteste vorweg zu sehen.
Zu sehen, da braucht sich was zusammen, da muss man irgendwie jetzt als Inlandsgeheimdienst einschreiten.
Aber auch Software, die in Richtung Hacking geht, das ausspionieren von Zielen, die man dann hacken kann,
was ja auch russische Geheimdienste sehr gerne machen im Ausland.
Also nochmal zusammengefasst, Desinformation, Zensur, Überwachung.
Gibt es denn auch Hinweise darauf, dass Russland über Vulkan tatsächlich auch zum Beispiel Angriffe auf Infrastruktur durchgeführt hat?
Also Attacken auf Infrastruktur, da gibt es viele Belege, dass die stattgefunden haben.
Sehr stark in der Ukraine, die Ukraine war für die russischen Geheimdienste im Prinzip ein Testfeld schon seit mindestens 2014, 2015 ist es dort zum ersten Mal gelungen,
dass russische Hacker tatsächlich ein Stromnetzlamm gelegt haben für einige Zeit und 2016 nochmal.
Also schon bevor dieser Krieg losging in klassischer Natur, Jahre vorher,
haben russische Hacker schon versucht, dort Chaos zu stiften, um einfach das Vertrauen in den Staat auch zu zerstören.
Spielen denn russische Cyber-Angriffe im jetzigen aktuellen Krieg gegen die Ukraine eine Rolle?
Ja, das spielen sie definitiv. Das haben ukrainische Cyber-Verteidiger auch gerade dokumentiert.
Ukraine's Cyber Security Authority says the cyber conflict with Russia is unprecedented,
describing it as the world's first hybrid war.
Und da sieht man ganz klar, es hat sich an der Häufigkeit was getan.

Also es wurden viel mehr Angriffe gestartet, einerseits gegen Infrastruktur, also wie Stromnetze, andererseits aber auch zum Beispiel gegen Medienunternehmen, gegen staatliche Institutionen, auf ganz unterschiedliche Weise am Anfang noch etwas ausgefuchster und ausgeklügelter und später dann ja eher relativ grob mit Programmen, die zum Beispiel einfach Zerstörung anrichten sollen,
die befallene Rechner einfach löschen und unbenutzbar machen.
Und es gibt auch Angriffe, die in zeitlichen Zusammenhang stehen mit konventionellen Angriffen.
Also die Ukraine sind da sehr deutlich in ihrer Einschätzung, dass sie sagen,
das ist auf jeden Fall eine Art von Hybriderkriegsführung.
Geht aus diesen Informationen, die ihr bekommen habt, hervor, wie solche Operationen abgelaufen sind?
Also Schritt für Schritt?
Das ist tatsächlich in den Dokumenten nicht beschrieben.
Es gibt zum Beispiel Programme, die zur Zielaufklärung mutmaßlich eingesetzt werden,
die die Ziele identifizieren, wie das auch im konventionellen Krieg mit Aufklärungsflugzeugen oder sowas passieren würde.
Und das gibt es im digitalen Raum, aber wir sehen natürlich nicht aktuell in das Handeln,
welche Informationen dann, wie für welchen Angriff genutzt wird.
Also Hinweise darauf gibt es nicht in den Dokumenten, aber vielleicht für jemand,
der keinen Einblick hat, wie muss man sich denn vorstellen, wie so ein Cyberangriff ablaufen kann, wenn man zum Beispiel ein Kraftwerk ins Visier nimmt?
Also wir haben mit einem Mann gesprochen, der zum Beispiel im Jahr 2015 schon dabei war,
als eine russische Hackergruppe mutmaßlich das Kraftwerk, in dem er arbeitete, angegriffen hat.
Und damals war das so, dass er eben vor einem Computer saß und plötzlich sich dem Auszeiger bewegte.
Und was willst du jetzt machen?
Was willst du jetzt machen?
Das ist eine Sekzine, was willst du jetzt machen?
Was willst du jetzt machen?
Was willst du jetzt machen?
Das ist eine Sekzine von 110 KV.
Und wie von Geisterhand und er nichts mehr dagegen tun konnte und der Mauszeiger dann nach und nach
sogenannte Umspannwerke abgeschaltet hat und man sozusagen live zuschauen musste, wie Fremde die Kontrolle übernommen haben
in diesem Netzwerk und dafür gesorgt haben, dass in Krankenhäusern, Kindergärten und so weiter der Strom ausgefallen ist.
Das ist wirklich, wirklich gespenstisch, wenn man so drüber nachdenkt.
Ich würde sagen, wir lassen das für eine kurze Pause sicken.
Danach stößt auch dein Kollege Frederik Obermeier zu uns und wir sprechen weiter über die verdeckten Aktionen
der Firma Vulkan und Russlands Cybercreation.
Auch hier bei uns in Österreich und Deutschland. Und wie das Ganze in einem Schlagabtausch zwischen Russland und im Westen enden könnte.

Bleiben Sie dran!
Was ich nicht nachvollziehen kann, ist, warum an jedem Unrecht immer ich schuld sein soll.
Ein Korruptionssinn.
Österreich hat in den letzten 30 Jahren viel über Klimaschutz gesprochen, aber zu wenig getan.
Die Politik verschläft die Klimakrise.
Die Behörden haben alles richtig gemacht.
Fehler vergisst man, statt daraus zu lernen.
So sind wir nicht. So ist Österreich einfach nicht.
Aber wie ist Österreich nicht?
So ist Österreich einfach nicht.
Aber wie ist Österreich dann?
Das wollen wir bei Inside Austria herausfinden.
Wir blicken auf die großen österreichischen Skandale.
Von Ibiza bis Ischgl.
Wir wollen wissen, wer dafür in der Politik die Verantwortung trägt.
Und wir schauen genau hin, wo Österreich über seine Grenzen hinaus mitmischt.
Vom Wirecard-Skandal bis zum Ukraine-Krieg.
Das ist Inside Austria von Standard und Spiegel.
Jeden Samstag eine neue Folge überall, wo es Podcast gibt.
Das heißt, dass sie vor allem in Russisch waren.
Haben wir einen russischsprachiges Team zusammengestellt.
Haben aber gleichzeitig auch die Unterlagen automatisiert übersetzt.
Und einem größeren Team, wo unter anderem die Washington Post, der Guardian und LeMond, beteiligt war.
Und dort vor allem die Cyber-Experten und die Russland-Expertinnen.
Was wir dann gemacht haben, wir haben erst mal geschaut in diesen Dokumenten.
Wo gibt es denn da Bezüge zur Wirklichkeit?
Sei es zum Beispiel die Namen von Mitarbeitern, Telefonnummern.
Finden wir davon Bezüge in der Realität.
Und haben die Unterlagen dann auch vertraulich mit IT-Expertinnen geteilt.
Haben sie auch einigen Geheimdiensten vorgelegt, eine Auswahl davon.
Und die kamen alle zu dem Schluss.
Die sind authentisch.
Es kam sogar in den letzten Tagen noch ein großer Durchbruch bei unsere Recherche.
Nämlich das Experten von Google, mit denen wir gesprochen haben.
Uns bestätigt haben, was bislang noch niemand wusste,
dass nämlich Google schon 2012 eine Verbindung von Vulkan,
also dieser Firma im Zentrum der Vulkan-Pfeils, zu einer Melwe namens Miniduke gezogen hat.
Google und Twitter wurden verabschiedet, um die Mauer zu koordinieren.
Die Mauer hatte nicht eine harte Kode, eine Kommandant-Control-Server-Adresse,
sondern sie hatte ein paar harte Kode Twitter-Accounts.
Und sie checkte Twitter für Informationen.
Die anderen zwei Dokumente haben Informationen über die politische Polizei von Ukraine
und die NATO-Memberschaft von Ukraine.

Es ist sehr interessant und wichtig, dass die Kontenten von diesen Mails und Dokumente generell related zu den Victim sind.
Sie haben auch die Firma Vulkan selbst ausfindig gemacht, war sie vor Ort?
Wir haben aber mit insgesamt mehr als 90 aktuellen oder frühere MitarbeiterInnen Kontakt aufgenommen.
Einige von denen haben auch mit uns gesprochen, haben auch Inhalte aus den Vulkan-Pfeils bestätigen können.
Wir haben auch einen Mitarbeiter, mit dem wir es sehr, sehr lange gesprochen haben,
der sich mittlerweile in den Westen abgesetzt hat, der uns auch erklärt hat,
dass er am Anfang dachte, dass die Firma NTC Vulkan so eine ganz normale IT-Firma wäre,
so ein Mittelständler, wie man es aus aller Herren Länder kennt.
Und er hat dann aber ziemlich schnell gemerkt, dass die Firma hinter dieser Fassade
in Wahrheit für russische Geheimdienste arbeitet.
Und hat deswegen gesagt, das kann er mit seinem Gewissen nicht vereinbaren,
hat deswegen dann Russland verlassen.
Genau das würde mich nämlich interessieren, weil du hast gesagt,
der konnte es mit seinem Gewissen nicht vereinbaren für so eine Firma zu arbeiten.
Wer sind denn die Menschen, die für Vulkan arbeiten?
Ich kann mir vorstellen, sie werden nicht unbedingt damit werben,
dass sie den Cyberkrieg für Protein durchführen sozusagen?
Ne, NTC Vulkan schaut nach außen hin erstmal aus wie eine ganz normale IT-Firma.
Wie eine IT-Firma, die unter anderem zum Beispiel für die Moskauer Börse,
aber auch die Sperrbank arbeitet, die auf ihrer Homepage als Kunden und Partner,
auch so Firmen wie Dell, IBM und andere Firmen, die wir so kennen,
die man auch erst nicht IT-Spezialist kennt, arbeiten.
Wenn man dann aber genauer hinschaut und das sehen wir auch eben in den Vulkan-Feis,
arbeiten sie für die entscheidenden russischen Geheimdienste,
nämlich den FSB, den SWR und die GRU.
Das sind aber Dinge, die sie nach außen hin natürlich nicht so an ihrer Homepage plakatieren,
mit der sie nicht so hausieren gehen, weil sie natürlich auch wahrscheinlich wissen,
dass sie damit ins Visier des Westens geraten können, denn das muss man schon aufsagen.
Gerade diese Geheimdienstzulieferer, diese Geheimdienstdienstleister
sind in den vergangenen Monaten zunehmend ins Visier westlicher Behörden geraten.
Die Amerikaner haben sehr, sehr viele dieser Firmen mittlerweile sanktioniert.
Wir wissen auch aus der Europäischen Union, dass es dort solche Überlegungen gibt,
diese Dienstleister vermehrt ins Visier zu nehmen, da man natürlich auch mittlerweile gemerkt hat,
es sind eben nicht nur die Geheimdienste, es ist nicht nur das Militär,
was den russischen Cyberkrieg führt, sondern diesen Zunehmend auch auf Dienstleister angewiesen.
Was sagen denn die Behörden in Europa und in Übersee?
Du hast sie schon angesprochen zu diesen Enthüllungen.
Ist man jetzt noch mehr alarmiert als vorher?
Die Behörden, also vor allem die Geheimdienste und Sicherheitsbehörden
sind ohnehin schon seit Jahren mittlerweile alarmiert.

Sie beobachten zunehmend, dass russische Hacker an allen Ecken und Enden versuchen,
in unsere Netze einzudrängen.
Ein hochrangiger BND-Funktionär hat auch vor kurzem mal bei einer Konferenz klargemacht,
dass wir uns darüber im Klaren sein müssen und auch nichts vormachen brauchen,
dass russische Hacker schon längst in Deutschland in der Netze sind.
Deswegen müssen wir auch davon ausgehen, dass es in Österreich nicht viel anders ist.
Und was wir aber jetzt hier durch die Vulkanpfeils gesehen haben,
ist das erste Mal so ein Schlüssellochblick.
Wir sehen das, was man bislang nur von außen gesehen hat,
wo man immer nur Spuren dieser Angriffe gesehen hat, sehen wir jetzt erstmals,
wie diese Infrastruktur für diese Angriffe gebaut wird, was das Ziel ist,
was man sich so als Zielsetzung setzt, was so der Wunschtraum der russischen Geheimdienste ist.
Das muss man sich vorstellen, wie so eine Art Wunschliste,
wo sie einmal aufgeschrieben haben, liebe Programmierer, das hätten wir gern, das wollen wir haben.
Bitte baut es, programmiert es.
Was steht denn da zu aller Obers auf dieser Wunschliste?
Auf dieser Wunschliste sind wir mehrere große Komplexe.
Wir sind zum einen den Komplex desinformationen.
Wir merken ja schon und das wird ja auch schon seit einiger Zeit mittlerweile kritisiert
und angemerkt, dass Russland nicht nur in Europa des Informationskampagnen
gigantischer Art fährt, sondern auch in den Vereinigten Staaten,
auch zunehmend in Afrika.
Was wir jetzt hier sehen, ist, dass es sich quasi so ein Super-Tool wünschen,
mit dem man möglichst schnell, möglichst viele Social-Media-Profile gründen, bauen kann,
die im besten Fall von Facebook, Twitter und Co. nicht so schnell entdeckt werden.
Dann sehen wir darüber hinaus, dass sie quasi so ein Tool sich wünschen,
zum Suchen nach Schwachstellen.
Also es muss man sich so vorstellen, dass sie sich eigentlich von einem Tool wünschen,
mit dem man das Internet und alle angeschlossenen Geräte weltweit scannt
und dann einfach mal schaut, was laufen denn,
auf welchen Servern zum Beispiel, was für Programme laufen denn da,
was für eine Software läuft da.
Wenn man nämlich das weiß, kann man auch gleichzeitig schauen,
ist die auf dem aktuellen Stand.
Wenn sie nicht auf dem aktuellen Stand ist, gibt es womöglich Schwachstellen.
Das sind dann genau die Punkte, wo angreifert,
wenn sie sich entscheiden, zum Beispiel eine gewisse Institution anzugreifen,
einfach nur sagen müssen, ah, okay, die haben den Server nicht abgedeitet,
da wissen wir, dass es dann quasi ein Exploit gibt, das nutzen wir, um dort einzudrängen.
Dann, was ein weiterer Aspekt ist, den wir sehen,
ist, dass quasi sich die russischen Geheimdienste und Militärs Informationskontrolle ausüben wollen.
Sie wollen zum Beispiel in besetzten Gebieten, wie man es ja jetzt auch in der Ukraine sieht,
verhindern, dass die Bevölkerung Zugang zum freien Teil des Internets hat.

Sie wollen kontrollieren, welche Webseiten sie sehen und welche nicht.
Und das haben wir jetzt auch mittlerweile aus den besetzten Gebieten in der Ukraine schon von mehreren Bewohnerinnen gehört,
dass sie von einem Tag auf den nächsten gemerkt haben,
sie können nicht mal Homepages besuchen.
Sie können ukrainische Nachrichten nicht mehr besuchen,
werden auf irgendwelche russischen Seiten umgeleitet.
Und das ist was, wo wir einfach merken, hier will Russland zunehmend tätig werden und verlassen sich da auf Vulkan, die nötige Infrastruktur aufzubauen.
Was unterscheidet denn die Operationen von Russland eben von jenen Europas oder den USA?
Auch in den USA gab es ein großes Überwachungsprojekt,
das ja mit etwas Noten aufgeflogen ist.
Was wir natürlich schon aufsehen, ist, dass Russland nicht der einzige Player ist.
Die Chinesen rüsten extrem auf die Vereinigten Staaten und ihre Verbündeten.
Da haben wir sie ja durch die Snowden-Files, die NSA-Files gelernt,
auch was sie für eine Werkzeug-Toolkit vor sich liegen haben.
Was wir bei Russland aber zunehmen sehen,
ist, dass russische Hackerangriffe zunehmend auch unser Leben, also unser alltägliches Leben beschäftigen.
Während man von amerikanischen Hackerangriffen relativ wenig mitkriegt,
ist es so, dass wir von russischen Hackerangriffen sehr, sehr viel mitbekommen.
Wir kriegen mit, wenn zum Beispiel beim MERSC
einen der größten Rädereien der Welt auf einmal die Software-Systeme ausfallen.
Wir kriegen mit, wenn auf einmal Satelliten-Kommunikation ausfällt.
Wir kriegen mit, wenn auf einmal Banken ihre Systeme herunterfahren müssen.
Weil all das sich auf entweder gezielte oder auch schiefgelaufene russische Hackerangriffe zurückführen lässt.
Wenn man da auf der anderen Seite schaut, im Westen, gab es sowas auch schon mal.
It's believed the US and Israel ordered a cyberattack
to slow down Iran's nuclear program.
Wo man versucht hat, Zentrifugen zu zerstören,
zur Atomanreicherung.
Das ist auch aus dem Ruder gelaufen und hat dann im Endeffekt dazu geführt,
dass dieses Tool oder diese Schadsoftware auf der ganzen Welt die Unwesen getrieben hat.
Seitdem sehen wir das aber vor allem bei russischer Melwe.
Würdest du sagen, Russland ist ein weitaus aggressiverer Player,
was die Cyberkriegsführung betrifft?
Derzeit sehen wir das Russland in diesem Bereich extrem aufrüstet.
Wir merken das aber auch an der offiziellen Kommunikation.
Russland versteckt es auch nicht, dass sie sagen,
sie sehen mittlerweile fünf Bereiche, wo sie Krieg führen.
Und zwar ist es auf dem Wasser, in der Luft, auf dem Land, im Weltall
und im Fünften des dann der Cyberspace, im Internet, wo wir alle zum Ziel werden können.
Wie gut ist denn Europa gerüstet gegen solche Cyberangriffe?

Ich fürchte leider nicht so gut.
Wir haben ja wirklich fast im Monatsrhythmus Angriffe, die nicht abgewert werden konnten.
Wenn man hier in Deutschland schaut, ist es mutmaßlich russischen Hackern gelungen,
bis in die IT-Infrastruktur des Bundestags vorzudringen
und dort sogar bis auf einen Rechner von unserer damaligen Bundeskanzlerin Angela Merkel.
Da muss man schon sagen, die Kanzlerin dürfte eines der gesichertsten IT-Infrastrukturen in Deutschland haben.
Wenn es selbst dort gelingt, dann möchte ich nicht wissen,
was wir sonst gar nicht sehen, weil es nicht kommuniziert wird oder weil es noch gar nicht aufgefallen ist.
Das sind tatsächlich nicht die besten Aussichten, die du uns da gibst.
Was würdest du denn sagen, was erwartet uns da noch in Zukunft?
Sind wir jetzt schon mittendrin in einem globalen Cyberkrieg oder ist das tatsächlich erst der Anfang?
Ich glaube, dass wir schon mittendrin sind.
Dass es jetzt noch ein verdeckter, ein geheimer Krieg ist,
der aber zunehmend Auswirkungen auf unser alltägliches Leben haben wird.
Ich hoffe auch, dass das zunehmend auch zu einer Diskussion in der Öffentlichkeit führt,
dass wir uns alle mehr Gedanken machen, wie können wir unsere Infrastruktur schützen,
wie können wir unsere eigene Handys, unsere Laptops schützen.
Und da dürfen wir nicht naiv sein, wir dürfen nicht sagen nur,
weil ich jetzt nur Frederik Obermeier bin, mich in Regierungsfunktionen,
bin ich nicht für Geheimdienst der Arbeit.
Trotzdem kann ich entweder absichtlich oder auch durch einen Unfall zum Ziel werden.
Und das kann natürlich für mein Leben extreme Konsequenzen haben,
wenn man sich mal überlegt, was wir mittlerweile auf unseren Laptops,
Handys und auch in der Cloud alle speichern.
Das fängt ja mit Familienbildern an, bis hin zu Bankunterlagen
und viel mehr, alles Dinge, die wir ja nicht in der Öffentlichkeit haben wollen.
Erwartest du, dass wir in Zukunft öfter von solchen Vorfällen hören
und dass es vielleicht auch zu einem Art Schlagabtausch kommt zwischen den Ländern?
Na ja, was wir schon sehen in den Vulkanfalls, ist so ein Spektrum,
was die Russen offenbar ins Visier genommen haben.
Also wir sehen ja zum Beispiel eben eine so eine Beispieldiagramm,
wo unter anderem ein Atomkraftwerk, ein mittlerweile stillgelegtes Atomkraftwerk
in der Schweiz eingezeichnet ist.
Ich glaube nicht, dass sie direkt das schon konkret im Visier hatten,
aber man sieht so ein bisschen die Dimension auf, was sie es abgesehen haben,
dass eben Energieversorgung von anderen Ländern ins Visier genommen werden.
Das ist ja auch was, was wir in der Ukraine schon vor dem Überfall gesehen haben
und auch seither immer wieder sehen, dass genau die Strom- und Wasserversorgung ins Visier genommen wird.
Aber denkst du, dass andere Länder zurückschlagen werden,
wenn solche Aktionen passieren?

Oder denkst du, man wird sich jetzt im Westen vor allem darum bemühen, solche Sachen abzuwehren?
Also zumindest sehen wir schon diese Diskussionen.
Dürfen westliche Geheimdienste, westliche Sicherheitsbehörden zurückschlagen,
wenn sie sich angegriffen fühlen oder Anzeichen dafür sehen?
Ich glaube, das ist jetzt vor allem eine Diskussion,
aber ich glaube schon, dass es in Zukunft immer mehr die Diskussion in den Behörden bestimmen wird
und dass wir uns darauf gefasst machen müssen, dass zunehmend auch zurückgeschlagen wird.
Und dann ist natürlich die Gefahr von so einer Eskalationsspirale.
Deswegen, ich hoffe, dass es nicht so weit kommt.
Ich hoffe, dass alle Seiten hier abrüsten,
einfach weil es für unser tägliches Leben natürlich verheerende Auswirkungen haben kann.
Hannes, nach all dem, was wir bisher gehört haben, geht es bei diesen Vulkanfalls wortwörtlich um Leben und Tod, nicht nur um irgendwelche Daten im Netz, die verschwinden und Computersysteme, die abgedreht werden.
Welches Risiko ist denn dieser Whistleblower, der sich ganz am Anfang bei dir gemeldet hat, eingegangen, den wir diese Enthüllungen zu verdanken haben?
Ich glaube, ein sehr großes Risiko.
Wir müssen davon ausgehen, dass, wenn jemand geheimnisse, russischer Geheimdienste verrät, dass diese Person als Verräter angesehen wird dort und dass Versuche unternommen werden, sie zu finden und dass man mit diesen Leuten nicht klimflich umgeht.
Das wissen wir seit Fällen wie Litvinenko oder Skripal, die auch noch im Ausland vergiftet wurden, nachdem sie ausgepackt hatten.
Während wir hier sprechen, erscheinen überall auf der Welt in verschiedensten Medien Berichte über diese Vulkanfiles und deine und eure Recherchen, hattest du denn kurz vor der Veröffentlichung
oder vielleicht auch heute noch, nochmals Kontakt zu deiner Quelle?
Weißt du, was aus dir geworden ist?
Nein, ich weiß nicht, was aus dieser Person geworden ist.
Und wenn ich es wüsste, dürfte ich es wahrscheinlich nicht sagen.
Hannes Munzinger, Frederik Obermeier, vielen Dank für eure Recherche.
Sehr gerne.
Großes Dankeschön auch an die vielen weiteren Kolleginnen, die an diesem Investigativ-Projekt beteiligt waren.
Auch der Standard hat dazu einiges recherchiert.
Alle Artikel finden Sie auf der Standard.at.
Und unsere Freunde vom Spiegel haben den Vulkanfiles auch eine eigene Podcast-Serie gewidmet.
Hören wir da mal rein.
Wir haben Menschen in der Ukraine getroffen, die angegriffen wurden.
Die Dokumente sind eine Warnung.
Was wir bei unserer Recherche über Russlands digitale Waffen erfahren haben, geht weit über die Ukraine hinaus.
Der Krieg im Internet hat längst begonnen und wir alle sind das Ziel.

Spannung pur.
Putins Krieg im Netz.
Finden Sie überall, wo es Podcasts gibt.
Ich verabschiede mich an dieser Stelle.
Mein Name ist Schold Wilhelm.
Sie bleiben aber am besten dran.
Denn gleich berichtet Ihnen mein Kollege Tobias Holub über die weiteren wichtigen Schlagzeilen und Nachrichten des Tages im Meldungsüberblick.
Wir sind gleich zurück.
Und ich bin David Renert. Im Standard-Podcast Rätsel der Wissenschaft gehen wir großen Fragen der Menschheit auf die Spur.
Wir fragen Wissenschaftlerinnen, was in schwarzen Löchern passiert, wo die Aliens bleiben und die Fusionskraftwerke und wo die Mathematik an ihre Grenzen stößt.
Rätsel der Wissenschaft jeden Mittwoch eine neue Folge.
Danke auch von mir an Schold und unsere Interviewpartner.
Ich bin Tobias Holub und ich erzähle Ihnen jetzt noch, was Sie heute sonst noch wissen müssen.
Erstens. Bei der Zeitungsverlegerin Eva Dichand dürfte es eine Hausdurchsuchung durch die Wirtschafts- und Korruptionsstaatsanwaltschaft gegeben haben.
Das haben mehrere Medien heute am Donnerstag berichtet.
Eva Dichand ist Herausgeberin der Gratis-Zeitung heute.
Sie ist verheiratet mit Christoph Dichand, dem Chefredakteur der Kronen-Zeitung.
Hintergrund für eine Hausdurchsuchung dürfte das Geständnis des ehemaligen Finanzministerium Generalsekretärs Thomas Schmid sein.
Laut dem Ö1-Mittagsjournal soll Eva Dichand bei den Veränderungen beim Stiftungsrecht lobiert haben
und im Gegenzug eine positive Berichterstattung über Sebastian Kurz versprochen haben.
Zu Redaktionsschluss dieses Podcasts um 13 Uhr hat es noch keine Stellungnahme von Eva Dichand gegeben.
Aktuelle Informationen lesen Sie immer auf derStandard.at nach.
In jedem Fall gilt für alle Beteiligten die Unschuldsvermutung.
Zweitens, der ukrainische Präsident Volodymyr Zelenski hat heute am Donnerstagmorgen zum ersten Mal eine Rede vor dem österreichischen Parlament gehalten.
Er hat sich dabei bedankt für die bisherige Hilfe aus Österreich, hat um weitere Unterstützung gebeten
und auch österreichische Parlamentarierinnen nach Kiev eingeladen.
Die Rede hat mit Applaus geendet.
Österreich war das vor vorletzte Land in der EU, das Zelenski ins Parlament eingeladen hat.
Nur in den Russland freundlicheren Ländern Ungarn und Bulgarien ist das sonst noch nicht passiert.
Und auch gegen die heutige Rede von Zelenski hat es Kritik gegeben.
Die Parlamentarierinnen der FPÖ sind geschlossen aus dem Plenum ausgezogen
und auch mehr als die Hälfte der SPÖ-Abgeordneten waren während der Rede abwesend.
Beide Parteien haben sich in der Vergangenheit schon gegen eine Zelenski-Rede ausgesprochen, weil sie meinen, dass sie der österreichischen Neutralität widersprechen würde.
Drittens. Die Austrian Airlines, kurz AWA, haben sich mit ihrer Belegschaft auf einen neuen

Kollektivvertrag geeinigt.
Die zuständige Gewerkschaft hat ein höheres Gehaltsplus verlangt, weil die Inflation zuletzt stark gestiegen ist
und die AWA hohe Gewinne gemacht hat.
Nun hat man sich auf eine Erhöhung geeinigt, auch wenn die genauen Details noch nicht bekannt sind.
In jedem Fall dürfte es dadurch aber keine Streiks am Wiener Flughafen während der Osterfeiertage geben.
Und vierten. Schaben, Sex und Zucker. Damit beginnt bekanntlich jede gute Geschichte.
Das könnten sich zumindest jene US-Forscherinnen gedacht haben, die zuletzt eine passende Studie veröffentlicht haben.
Der Hintergrund zur Bekämpfung von Küchenschaben, Aka, Kaka laken,
werden schon seit vielen Jahren fallen eingesetzt, die mit Zucker gefüllt sind.
Das Problem? Kaka laken setzen bei der Paarung ein körpereigenes und zuckerhaltiges Sekret ein, um ihre Angebieteten anzulocken.
Und wegen der vielen Zuckerfallen finden Schaben Weibchen, das mittlerweile so gar nicht mehr anzieht.
Und die Lösung? Kaka laken Männchen haben den Anteil des betroffenen Zuckers in ihrem Sekret reduziert
und, Zitat, ihre Vorspielzeit von 4 auf 2 Sekunden reduziert, damit der Zucker weniger Zeit hat, Wirkung zu entfalten.
Die Forscherinnen sagen, dass man mit diesen Erkenntnissen jetzt die Schädlingsbekämpfung optimieren kann.
Ich sage dazu Evolution in a nutshell.
Alles weitere zum aktuellen Weltgeschehen lesen Sie wie immer auf der Standard.at
Und jetzt habe ich noch einen besonderen Hörtipp für Sie.
In der aktuellen Folge von unserem Schwester-Podcast Besser Leben geht es darum, wie man wirklich glücklich wird
und zwar mit wissenschaftlicher Unterstützung.
Dabei war nämlich auch eine neue Standard-Podcast-Kollegin, die Sie in Zukunft öfter hören können und wenn Sie über die und Ihren neuen Podcast mehr wissen wollen, dann hören Sie fürs Erste am besten gleich bei Besser Leben rein.
Überall, wo es Podcasts gibt.
Falls Sie uns noch irgendetwas sagen möchten, dann schreiben Sie gerne eine Mail an podcast.at
und wenn Ihnen diese Folge von Thema des Tages gefallen hat, dann abonnieren Sie uns am besten gleich auf Ihrer liebsten Podcast-Plattform.
Wenn Sie uns unterstützen möchten, können Sie ein Standard-Abo abschließen oder ein Premium-Abo auf Apple Podcasts.
Alle Infos finden Sie in den Show-Notes.
Ich bin Tobias Holop, danke fürs Zuhören und bis zum nächsten Mal.
Besser Leben, jeden Donnerstag eine neue Folge.