

Hackeraanvallen: eindelijk veilig op het blockchain-internet - of toch niet?

**De berichten over hackeraanvallen nemen elke dag toe in het nieuws. Deze algemene noodtoestand maakt de roep van het publiek elke dag luider: Er moet iets aan gedaan worden! In kringen van experts lijkt men het eens te zijn: Het nieuwe internet moet gebaseerd zijn op de zogenaamde blockchaintechnologie. Maar wat zit er achter het begrip “blockchain” en is het nieuwe internet Web 3.0 echt veilig? De eerste voortekenen voorspellen niet veel goeds.**

Hackeraanvallen: eindelijk veilig op het blockchain-internet - of toch niet?

Elke dag nemen in het nieuws de berichten over hackeraanvallen, cyberafpersing en meer toe. Geen doelwit wordt overgeslagen: Bedrijven, luchthavens, overheden, ziekenhuizen, oliepijpleidingen, scholen... Allemaal worden ze op dezelfde manier getroffen door de huidige cyberaanvallen.

Uit internationaal marktonderzoek blijkt dat elke tweede organisatie de afgelopen drie jaar het slachtoffer is geweest van een succesvolle cyberaanval. Het is dus een probleem dat ons allemaal aangaat!

In 2023 hebben zogenaamde ransomware-aanvallen nu al een maximum bereikt, hoewel het jaar nog niet eens is afgelopen. Bij een ransomware-aanval worden de computers van de slachtoffers versleuteld en alleen tegen betaling van losgeld weer ontsleuteld. Afhankelijk van de grootte van het bedrijf vraagt deze vorm van afpersing bedragen variërend van enkele honderdduizenden tot vele miljoenen. De eigenaars van de IT-systemen kunnen dan afwegen wat goedkoper is: IT-specialisten betalen die veel tijd nodig hebben om de schade te herstellen, het geëiste bedrag betalen of meteen het faillissement aanvragen. In veel gevallen is het het gemakkelijkst om het geldbedrag over te maken in cryptovaluta, en zo blijft de georganiseerde misdaad zich voor onze ogen uitbreiden.

Deze algemene noodtoestand maakt de publieke eis elke dag luider: Er moet iets aan gedaan worden! Het kan zo niet doorgaan! We leven tenslotte in een gedigitaliseerde maatschappij en wanneer kritieke infrastructuren zoals ziekenhuizen worden lamgelegd door anonieme hackers, kan dit levensbedreigend worden. Elke kritische waarnemer van de gebeurtenissen stelt zich echter de vraag: Zitten er echt individuele criminelen achter deze grootschalige hackeraanvallen? Zijn ze ongrijpbaar ondanks alle inspanningen van inlichtingendiensten en alomtegenwoordige internetsurveillance? Of zijn de aanvallers elitegroepen die doelbewust de verontwaardiging onder de bevolking aanwakkeren om hen ontvankelijk te maken voor een nieuw soort internet? Zo ja, wat zijn de doelen van deze handelende personen en wat voor nieuw internet proberen ze te creëren? Er wordt in vakkringen al veel gesproken over de volgende generatie internet. Het zogenaamde Web 3.0. Daaronder wordt een nieuw internettijdperk bedoeld dat gebaseerd is op volledig nieuwe principes en dat zo fraudebestendig zou moeten zijn dat het niet meer gehackt kan worden. Hoe kan dat werken?

Iedereen lijkt het erover eens te zijn dat het nieuwe internet gebaseerd moet zijn op de zogenaamde blockchaintechnologie. Vandaag wordt ons het onmogelijke beloofd: Meer gegevensbescherming, meer decentralisatie en onafhankelijkheid van de grote data-octopussen zoals Google, Microsoft, Facebook en Co. Op dit punt zal ik als voorbeeld fragmenten citeren uit een artikel van tagesschau.de: Het Web 3.0 wordt momenteel omringd door een soort vrije geest. Geen staatscontrole, geen toezicht - iedereen kan meedoen. (...) Het zou een netwerk zijn dat, volgens de ideeën van veel Silicon Valley meesterbreinen, toebehoort aan de gebruikers. Een gedecentraliseerd web gebaseerd op de zogenaamde blockchain. Dit zou het kunnen veranderen in een digitale lijst: Iedereen kan er een stukje van in bezit nemen. Het zou niet moeten toebehoren aan Tech bedrijven zoals Google of Facebook, noch aan banken of politieke systemen.

Hebben we het goed gelezen? Uitgerekend uit Silicon Valley, waar bijna alle grote Amerikaanse IT-bedrijven gevestigd zijn, komt het voorstel om een totaal ongecontroleerd internet te creëren dat niet langer aan de techgiganten toebehoort? Zijn ze opeens zo altruïstisch geworden en willen ze hun machtsmonopolie opgeven? Nauwelijks... Hier vermoed je al dat er niets goeds op ons afkomt.

Maar hoe werkt blockchaintechnologie? Zonder er diep op in te gaan, laat het volgende feit de oren spitsen: Heel vereenvoudigd gezegd is blockchaintechnologie gebaseerd op het principe dat een blok gegevens altijd naar alle computers in het blockchainnetwerk wordt gestuurd en dus op zoveel plaatsen is dat het theoretisch niet meer veranderd of gemanipuleerd kan worden. Het is verspreid over te veel apparaten om gewist te kunnen worden. Tegelijkertijd werkt de technologie ook als een ketting. Elke schakel van de gegevensketen is een permanente en transparante registratie. Dus voor altijd opgeslagen. Natuurlijk wordt ons verzekerd dat het allemaal anoniem en onkraakbaar is, enz. Maar is dat echt zo?

Iedereen die zich verdiept in blockchaintechnologie zal zonder twijfel ontdekken: deze technologie kan worden gebruikt voor de bevrijding of de totale verslaving van de mensheid. Het hangt er maar vanaf wie het controleert! Het huidige internet heeft ook een enorm potentieel voor de mensheid. Het probleem is dat het gecontroleerd en gecensureerd wordt door handelende personen die niet het welzijn van de mensheid voor ogen hebben, maar haar totale controle en onderwerping! Hetzelfde principe zal van toepassing zijn op Web 3.0. Hoe groot het potentieel van de blockchain ook zou kunnen zijn, en waarom het momenteel veel technologiefreaks geestdriftig maakt: In de handen van het WEF, de EU, de VN, de Gates Foundation en andere centrale handelende personen zal Web 3.0 een nachtmerrie worden! Want deze instellingen pleiten vurig voor een digitale identiteit voor alle burgers ter wereld. Een digitale identiteit bevat ALLES wat je ooit hebt gedaan, gekocht en ondernomen. Blockchain technologie lijkt gemaakt te zijn voor totale controle - de transparante burger, de totale controle van de mensheid tot in het kleinste detail - en zal daarom, in de verkeerde handen, het grootste gevaar worden voor de vrije mensheid!

Hoe ver zijn deze plannen gevorderd? Het feit dat drie blockchainpioniers, Nikolai Mushegian, Tiantian Kullander en Vyacheslav Taran, in 2022 al “toevallig” om het leven zijn gekomen - binnen slechts vier weken - voorspelt niets goeds. Één van de blockchainontwikkelaars schreef enkele uren voor zijn verdwijning over een vermeend complot van de CIA, Mossad en pedofielen uit de elite dat zij op hem jaagden. “Ze gaan me doodmartelen!” schreef hij op Twitter. Wat betekent dit allemaal? Zijn de blockchainontwikkelingen van deze genieën gestolen en worden ze nu verwerkt voor wereldwijde plannen? Daarover kunnen we alleen maar speculeren.

Samenvattend moeten we zeggen of het nu Web 3.0, blockchain of wat dan ook is ... dat de ene crisis na de andere kunstmatig zal worden opgeroepen om ons ontvankelijk te maken voor de nieuwe controletechnologie. Financiële crashes zullen worden gebruikt om digitaal centraal bankgeld te introduceren, cyberaanvallen om een transparant internet te creëren,

plandemieën om de mensheid te decimeren door middel van gen-veranderde mRNA vaccinaties, etc.

In het licht van deze ontwikkelingen is het natuurlijk om in berusting te vervallen.

En toch weten we dat elke ophelderingactie ons een stuk dichter bij het doel van een vrije mensheid brengt:

Stuur daarom deze video naar uw vrienden en kennissen en doe met ons mee om elke knechtende digitalisering te trotseren! Wij zijn het volk!

**door es.**

**Bronnen:**

Blockchain und Web 3.0
( Blockchain en Web 3.0)
<https://www.ibm.com/de-de/topics/blockchain>
<https://www.bitpanda.com/academy/de/lektionen/wie-funktioniert-eine-blockchain/>
<https://www.avast.com/de-de/c-web-3-0>

Die Cyber-Bedrohungslage
(De cyber-bedreigingstoestand)
<https://sosafe-awareness.com/de/ressourcen/reports/human-risk-review/>

Silicon Valley
<https://www.tagesschau.de/ausland/silikon-valley-web3-101.html?xing_share=news>

Digitales Kontrollnetz
( digitaal controlenet)
<https://www.expresszeitung.com/ausgabe-51-digitales-gefaengnis-teil-1-2/ez10051.1>

Blockchain-Pioniere kommen ums Leben
( Blockchain pioniers komen om het leven)
<https://dailypost.ng/2022/11/30/crypto-moguls-taran-kullander-mushegian-die-in-four-weeks/>

**Dit zou u ook kunnen interesseren:**

#PriveModeraat - [www.kla.tv/PriveModeraat](https://www.kla.tv/PriveModeraat)

#Hacker - [www.kla.tv/Hacker-nl](https://www.kla.tv/Hacker-nl)

#Ontwikkeling - [www.kla.tv/Ontwikkeling](https://www.kla.tv/Ontwikkeling)

#Techniek - [www.kla.tv/Techniek](https://www.kla.tv/Techniek)

**Kla.TV – Het andere nieuws ... vrij – onafhankelijk – ongecensureerd ...**

* wat de media niet zouden moeten verzwijgen ...
* zelden gehoord van het volk, voor het volk ...
* nieuwsupdate elke 3 dagen vanaf 19:45 uur op [www.kla.tv/nl](https://www.kla.tv/nl)

Het is de moeite waard om het bij te houden!

**Gratis abonnement nieuwsbrief 2-wekelijks per E-Mail
verkrijgt u op:** [**www.kla.tv/abo-nl**](https://www.kla.tv/abo-nl)

**Kennisgeving:**

Tegenstemmen worden helaas steeds weer gecensureerd en onderdrukt. Zolang wij niet volgens de belangen en ideologieën van de kartelmedia journalistiek bedrijven, moeten wij er elk moment op bedacht zijn, dat er voorwendselen zullen worden gezocht om Kla.TV te blokkeren of te benadelen.

**Verbindt u daarom vandaag nog internetonafhankelijk met het netwerk!
Klickt u hier:** [**www.kla.tv/vernetzung&lang=nl**](https://www.kla.tv/vernetzung%26lang%3Dnl)

*Licence:  Creative Commons-Licentie met naamgeving*

Verspreiding en herbewerking is met naamgeving gewenst! Het materiaal mag echter niet uit de context gehaald gepresenteerd worden.
Met openbaar geld (GEZ, ...) gefinancierde instituties is het gebruik hiervan zonder overleg verboden.Schendingen kunnen strafrechtelijk vervolgd worden.