KEN JEBSEN < HTTPS://ANONLEAKS.NET/CATEGORY/OPTINFOIL/KEN-JEBSEN/>

OPTINFOIL < HTTPS://ANONLEAKS.NET/CATEGORY/OPTINFOIL/>

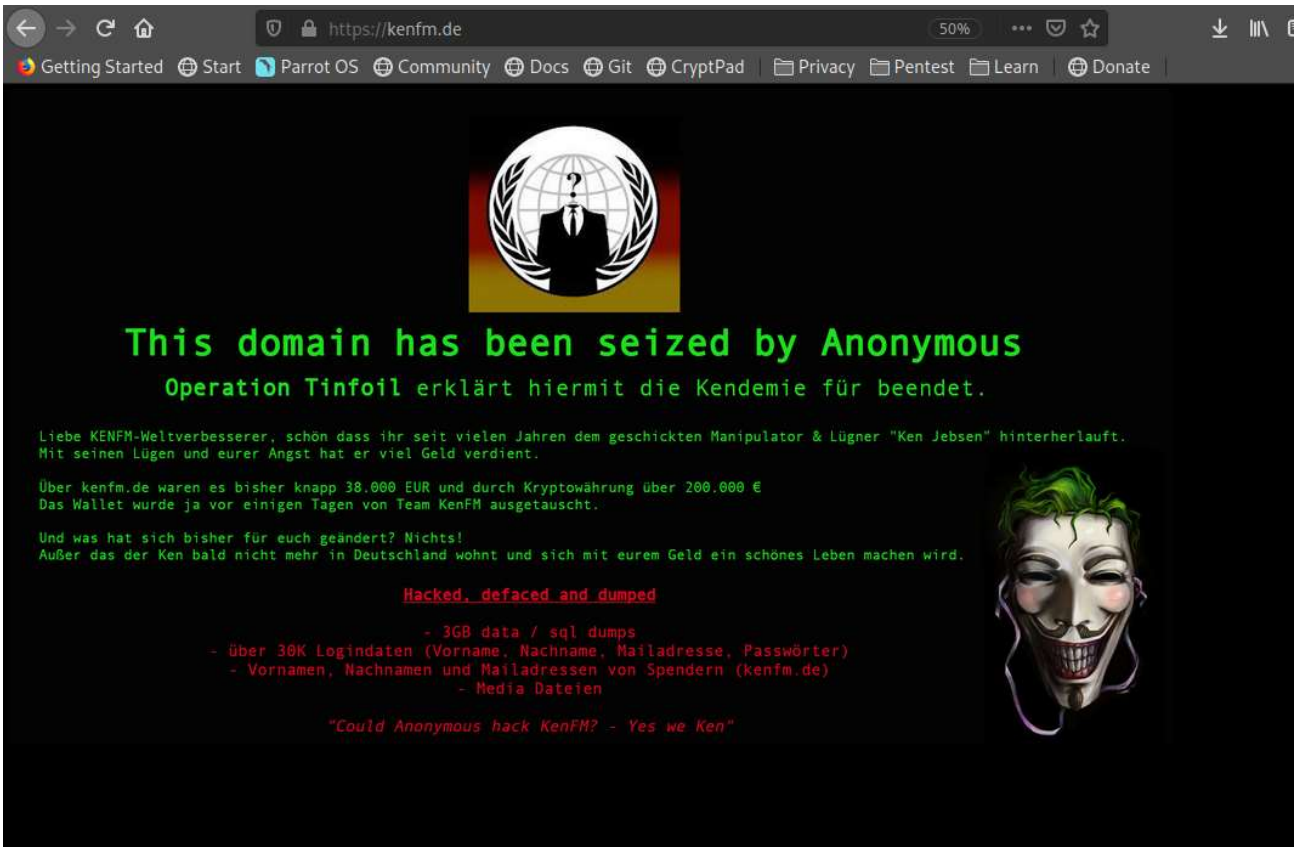
KennotFM: Details zu Hack und Defacement

Da der Angriffsvektor bei KenFM dicht ist, können wir auch verraten, wie es zu dem Hack kam.

Von AnonLeaks < https://anonleaks.net/author/anonroot2/>

13. Juni 2021, 16:28 Uhr < https://anonleaks.net/2021/optinfoil/kennotfm-details-zu-hack-und-defacement/>

83 Kommentare < https://anonleaks.net/2021/optinfoil/kennotfm-details-zu-hack-und-defacement/#comments> | Lesezeit: 7 Minuten

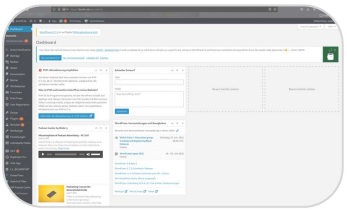


Gestern wurde KenFM.de, die Website von Ken Jebsen, von Anonymous gehackt. Wir berichteten.

Light Dark

Auch interessant:

Could Anonymous hack kenfm.de? – Yes we Ken! < https://anonleaks.net/2021/optinfoil/could-anonymous-hack-kenfm-de-yes-we-ken/>



Weil so viele gefragt haben und so viel spekuliert wurde, beleuchten wir in diesem Beitrag einmal, wie die Anons vorgingen, die Ken Jebsen gehackt haben. Denn wie immer bei Anonymous: alles wird dokumentiert.

Wenn man Hack und WordPress liest, wird zunächst immer auf veraltete Plugins geschlossen. Das war in diesem Fall nicht der Angriffsvektor, obwohl es veraltete Plugins gab.

KenFMs Site wurde in den vergangenen Monaten, Jahren eigentlich, immer mal wieder nebenher gescannt. Geht ja schnell und frisst kein Brot. Beim letzten Scan fand sich eine **Stored-XSS-Lücke < https://de.wikipedia.org/wiki/Cross-Site-Scripting>** (Stored Cross Site Scripting) mit CVE-Nummer (CVE= **Common Vulnerabilities and Exposures < https://de.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures>**) in einem Plugin, und so etwas weckt immer Interesse. Aber die war nicht der Grund, warum Ken Jebsen gehackt werden konnte, deswegen gehen wir darauf mal nicht näher ein. Sie führte letztlich nur dazu, dass man sich nochmal intensiver mit der Seite beschäftigte.

Und man wurde fündig: Es waren eine Datei namens database.sql (ein vollständiger Dump der MySQL-Datenbank) und ein Zip-Archiv mit einem Dateibackup der WordPress-Installation direkt über den Browser downloadbar. Die SQL-Datei konnte man zum Beispiel über den Link *https://kenfm.de/database.sql* herunterladen.

Ein klarer Fehler des Admins des Servers bzw. der Seite. Doch nicht der einzige.

Somit hatte man schon alle Daten aus einem Backup vom 01.06.2021, das war das Datum des letzten Beitrags im Dump. Und der Dump an sich war schon spannend mit all den User-Daten und Spendern, denn auf KenFMs WordPress hatte es mal eine Funktion zum direkten Spenden gegeben. Dieser Dump mit persönlichen Daten tausender Nutzer lag wenig DSGVO-konform frei zugänglich auf dem Server. Auch das wäre wieder etwas für eine Datenschutzbehörde.

Light Dark

Doch interessant ist es auch immer, die Dateien zu durchforsten, die man findet. Dabei fiel auf, dass bei einem der Plugins eine Datei installer.php ebenfalls frei zu erreichen war.

Sicher hätte man langwierig die gesalzenen und gehashten Passwörter der WordPress-User cracken können, aber gesalzen und gehasht bedeutet, die Passworte lagen nicht im Klartext vor, sondern hätten langwierig "bearbeitet" werden müssen, und das ohne jede Gewissheit, dass sie überhaupt crackbar waren. Aber mit einer installer.php konnte man arbeiten.

Vor allem weil die installer.php zum Plugin "Duplicator Pro" gehörte, einem Plugin, dass dazu dient, WordPress-Installationen zu klonen, umzuziehen oder ein Backup anzufertigen. Und mit der installer.php konnte man eben auch eine Installation wiederherstellen.

Die Anons nutzten den erbeuteten Dump und die Dateien, um auf dem Server von KenFM eine Spiegelinstallation in einem unverdächtigen Unterverzeichnis vorzunehmen. Im Grunde installierten sie also dasselbe WordPress mit den Inhalten vom 01.06. nochmals auf Kens eigenem Server.

< https://anonleaks.net/wp-content/uploads/2021/06/2shadow00.png>

< https://anonleaks.net/wp-content/uploads/2021/06/2shadowinst0.png>

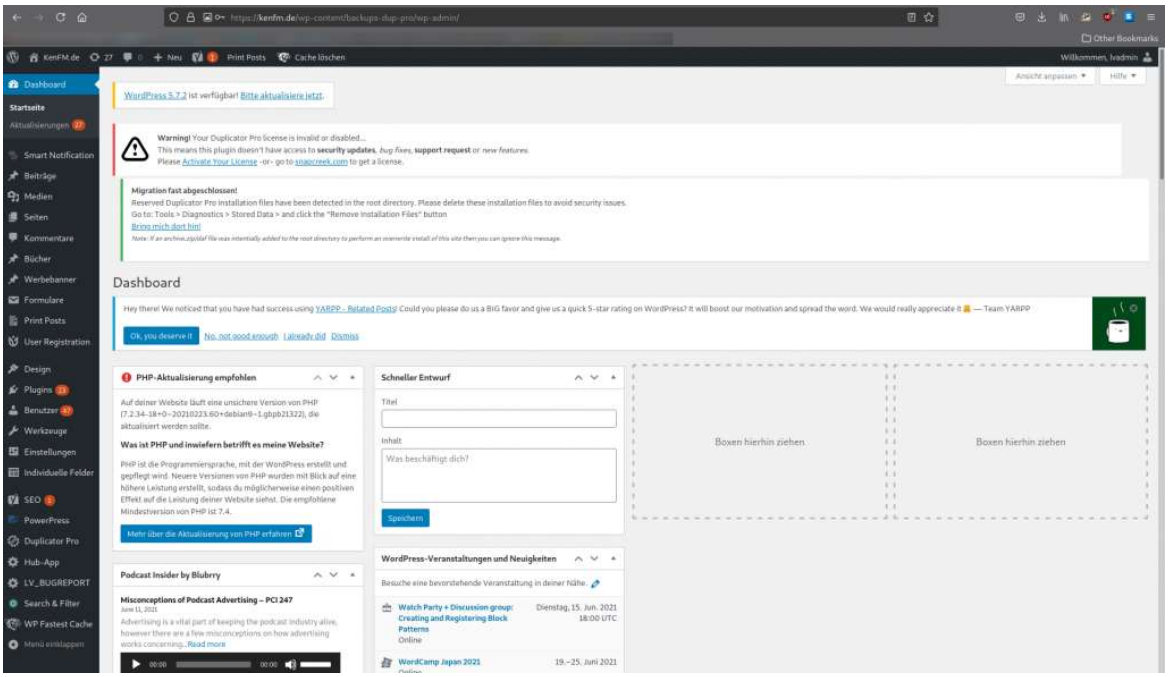
Man beachte das Verzeichnis in der Adresszeile des Screenshots.

Eine Herausforderung bei Spiegelinstallationen ist die Datenbank. Man muss dafür Sorge tragen, dass die Installation nicht auffällt und die aktive Datenbank nicht überschrieben wird. Eine Änderung des Tabellenpräfixes für Tabellennamen, die aus wp_users beispielsweise wpanon_users gemacht hätte, wäre sofort aufgefallen, wenn jemand einen Blick in die Datenbank geworfen hätte. Dies verbot sich also.

Light Dark

Gut bei Duplicator Pro ist, dass das Tool auch zum Umziehen von WordPress-Installationen genutzt werden kann. Deswegen kann man einen abweichenden Datenbank-Host, also einen anderen Server, angeben. Die Anons rekonstruierten also die WordPress-Dateien in ein Unterverzeichnis bei Ken, die Datenbank jedoch auf einen eigenen Server. Problem gelöst. Und da die Datenbank auf ihrem eigenen Server lag, konnten sie die Passwort-Hashes der Admins in der Datenbank einfach gegen eigene austauschen.

Login in die Spiegelinstallation ging also problemlos. Man hatte ein Login in ein "zweites" WordPress in einem Unterverzeichnis (im folgenden Bild gut zu sehen).



KenFM: WordPress Dashboard Spiegelinstallation mit Adminrechten

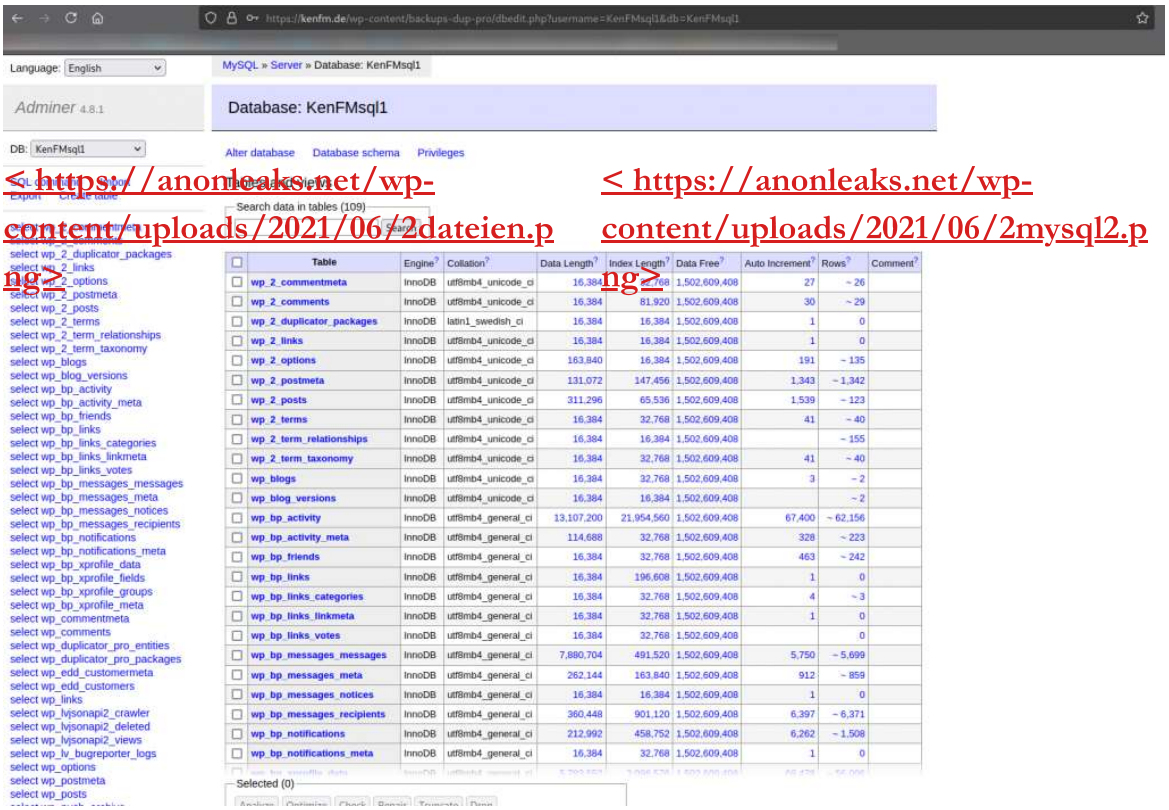
Der nächste Schritt: Die Installation eines File-Manager-Plugins. Damit kann man sich die Dateien auf dem gesamten Server ansehen, sie herunterladen und neue hochladen. Darüber bekam man Zugriff auf die Datei wp-config.php, in der sich die Zugangsdaten für die MySQL-Datenbanken befinden.

Light Dark

Filemanager

wp-config.php mit MySQL-Zugangsdaten

Nun konnte man direkt auf die Datenbank zugreifen. Adminer, ein Datenbank-Management-System (DBMS) half dabei.



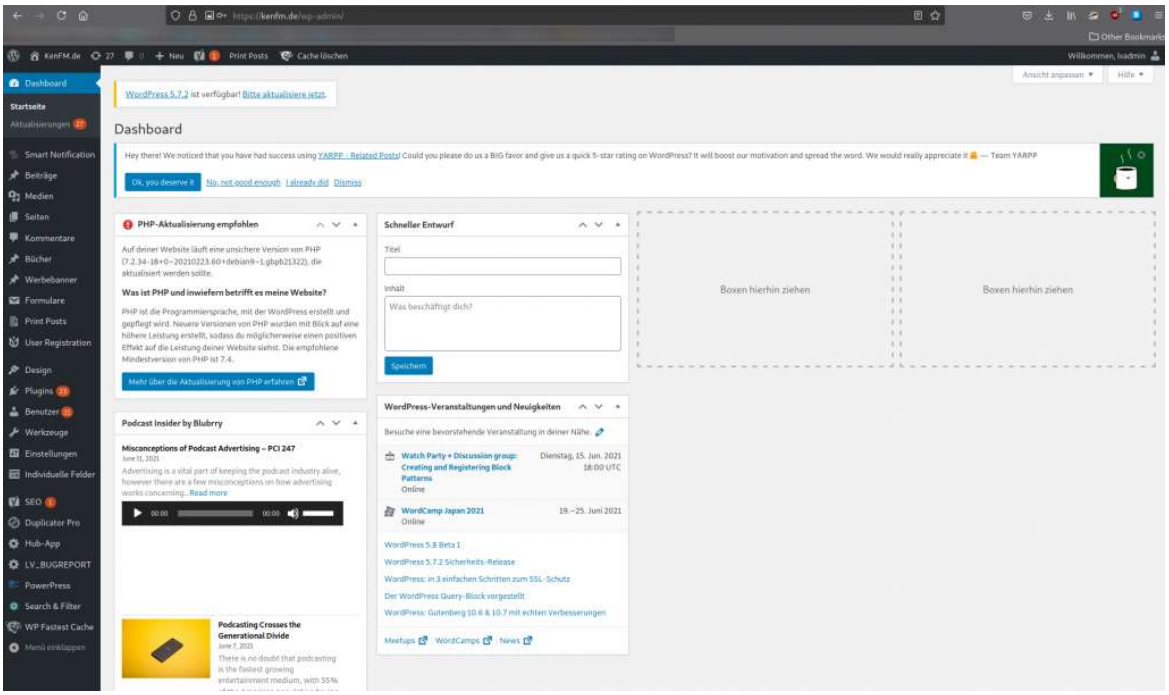
< https://anonleaks.net/wp-content/uploads/2021/06/2dateien.png>

< https://anonleaks.net/wp-content/uploads/2021/06/2mysql2.png>

KenFM: von Anons installiertes Adminer DBMS

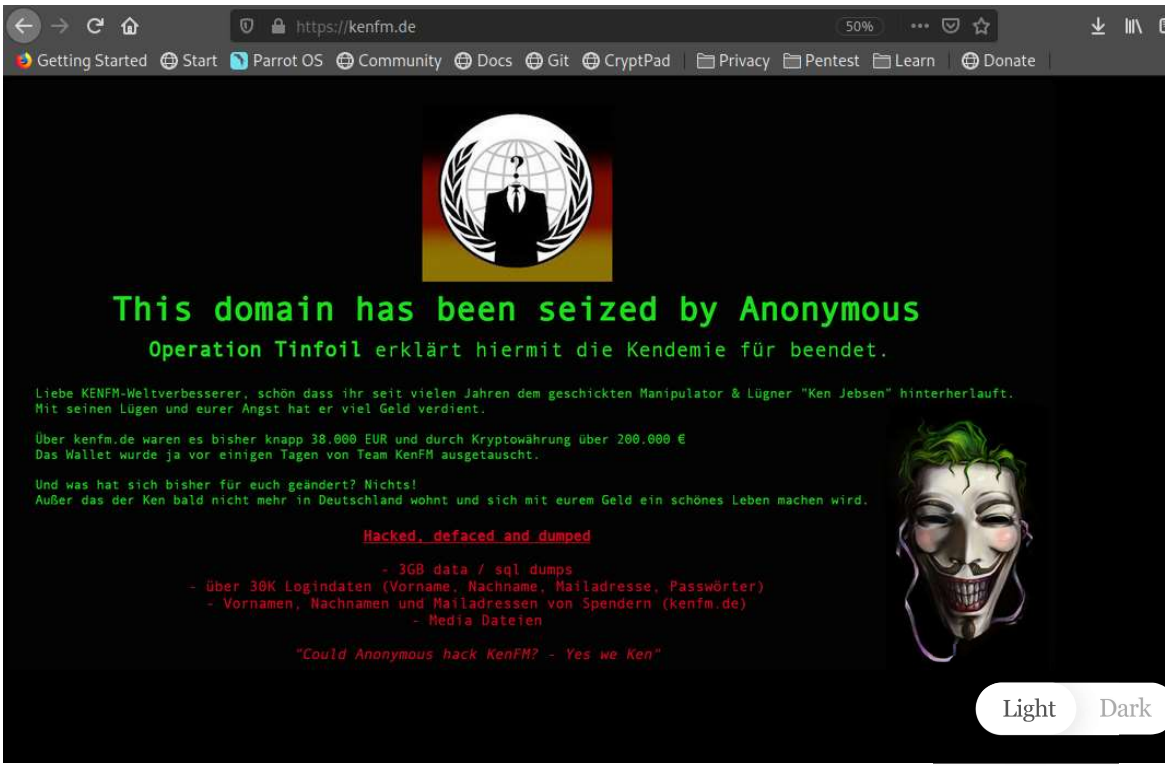
Nun konnte man auch hier Kens Admin-Passwort-Hash gegen den eigenen austauschen – und zack – man hatte Administratoren-Zugang im Live-System von KenFM. (Die URL in der Adresszeile: hier direkt /wp-admin, also ohne Unterverzeichnis, Live-System.)

Light Dark



KenFM: WordPress Dashboard Live-Site mit Adminrechten

Eigentlich hatten die Anons vor, mit der Seite ein bisschen zu spielen. Man hatte die Adresse des Bitcoin-Wallet schon gegen das eigene ausgetauscht. Aber sehr schnell wurde klar, dass dies zu auffällig sein würde. Die Kens und Barbies, die sich auf dem Server herumtreiben, sie sind zu aufmerksam. Also entschied man sich für Full Wipe & Defacement. Die Dateien, die Datenbank, alles wurde gelöscht und nur der kleine Anonymous-Gruß zurückgelassen.



Was lernt man daraus? Geduld, Hartnäckigkeit und vor allem eine gute Portion Kreativität und Teamwork unter guten Leuten zahlen sich immer aus. Anonymous hat das alles im Überfluss.

An dieser Stelle auch mal ein Wort an diejenigen, die jetzt darauf beharren, dass Anonymous keine Medien angreift. Diese ungeschriebene Regel existiert tatsächlich: Never attack the media. Aber wurde sie hier gebrochen? Der Begriff "Medium" ist vielschichtig, bei Anonymous sind damit journalistische Medien gemeint. Journalistische Medien halten sich normalerweise an besondere Standards wie Unabhängigkeit in der Berichterstattung, wahrheitsgetreue Berichterstattung, vor allem aber neutrale Berichterstattung.

Ein Medium entspricht nicht journalistischen Standards, wenn es berichtet, was eine Gruppe gerne hören möchte, sondern wenn es genau eben auch das berichtet, was diese Gruppe nicht hören möchte, weil es die Wahrheit ist. Doch wer definiert, was die Wahrheit ist? Das wäre ein schwieriges Kriterium.

Im Falle von Ken Jebsen ist es aber eigentlich recht einfach. KenFM ist direkt und unmittelbar mit der Person Ken Jebsen verbunden. Und Ken Jebsen hat sich bereits vor Jahren politisch positioniert. Dies hat er auch im vergangenen Jahr weitergeführt, indem er auf Querdenken-Bühnen auftrat und politische Reden hielt. Nicht als Kayvan Soufi-Siavash, als Privatmann, sondern als Ken Jebsen, KenFM. Welchen anderen Journalisten der gängigen Medien könnt ihr nennen, der das tat? Oder der das in einem Video tat? Einen noch? Zwei?

Ken Jebsen hat für viele Anons den Pfad journalistischer Neutralität verlassen. Er hat den Pfad journalistischer Integrität verlassen. Die Tatsache, dass sein Kanal von YouTube wegen medizinischer Falschinformationen gesperrt wurde, zeigt, dass er den Pfad journalistischer Wahrheit verlassen hat.

Journalist ist man nicht, wenn man einen Presseausweis hat. Heutzutage scheint jeder dahergelaufene Bauer, Tee, Nehrling oder Haintzelmann irgendwie an einen Presseausweis zu kommen. Sind die deswegen alle vor dem Angriff durch Anonymous geschützt? Wäre es dann für Schiffmann und Eckert nicht einfach gewesen, einen Blog aufzumachen, Presseausweis zu malen und zu sagen: "Bin jetzt journalistisches Medium" und Anonymous hätte zurückgezuckt? Könnte Querdenkens Ballweg nicht einfach sagen: "Bin jetzt Zeitung"?

Ganz so einfach darf man es sich nicht machen. Und ganz so undifferenziert darf man es nicht betrachten.

Und wo ist die Unterschied zwischen den Schiffmanns und Jebsens und den Reichelts und Poschards dieser Welt? Ganz einfach: letztere stehen nicht auf Bühnen und ihr Name ist nicht untrennbar mit ihrer Zeitung verbunden. Verbunden ja aber eben nicht untrennbar. Man kann von BILD und Welt und ihrem Geschreibsel halten, was man will, aber Reichelt und Poschard stehen nicht vor hunderten oder tausenden von Querdenkern und stacheln diese persönlich an. Und Julian Reichelt ist nicht BILD und Ulf Poschard ist nicht Welt, auch wenn sie das gerne in ihrer überbrodelnden Eitelkeit von sich glauben mögen. Ja, Springer ist dicht dran, jeden Funken journalistischer Integrität zu verlieren, nicht zuletzt auch durch die beiden Personen. Aber noch ist es nicht so weit. Wenn es so weit ist, merken die es als erstes.

Ken Jebsen ist KenFM. KenFM ist Ken Jebsen. Und Ken Jebsen ist politischer Agitator. Und damit zählt KenFM für sehr viele Anons nicht zu den geschützten Medien. Klar soweit?

Also auf zum nächsten – oder doch nicht? Man wird sehen.

So, und was macht man nun mit den Daten der knapp 39.000 Schwurbler, die sich regelmäßig von Ken Jebsen berieseln lassen und das Geschwurbel von dem auch noch für Journalismus halten?

An den Verfassungsschutz weiterreichen? Sicher nicht. Die Schlapphüte sollen mal schön selbst was leisten. Wäre ja mal ein Novum. Neue Befugnisse haben die Regierungsparteien ihnen ja verpasst – und das ist in mehr als einer Hinsicht sehr bedenklich. Aber Befugnisse haben nichts mit Kenntnissen und Wissen zu tun. Es bleiben Beamte. Also nö. Bringt nichts.

Journalisten Zugang gewähren? Also an echte, nicht an Kens, Stefans, Rüdigers oder Elijahs? Ja, das schon. Die sollen einfach mal schauen, ob sie wen kennen.

Und sonst? Mal schauen. Anonymous fällt immer was ein. Immer mal was Neues. Das unterscheidet uns von den … ach, lassen wir das.

← Could Anonymous hack kenfm.de? – Yes we Ken! < https://anonleaks.net/2021/optinfoil/could-anonymous-hack-kenfm-de-yes-we-ken/>

Light Dark

Hoch ↑