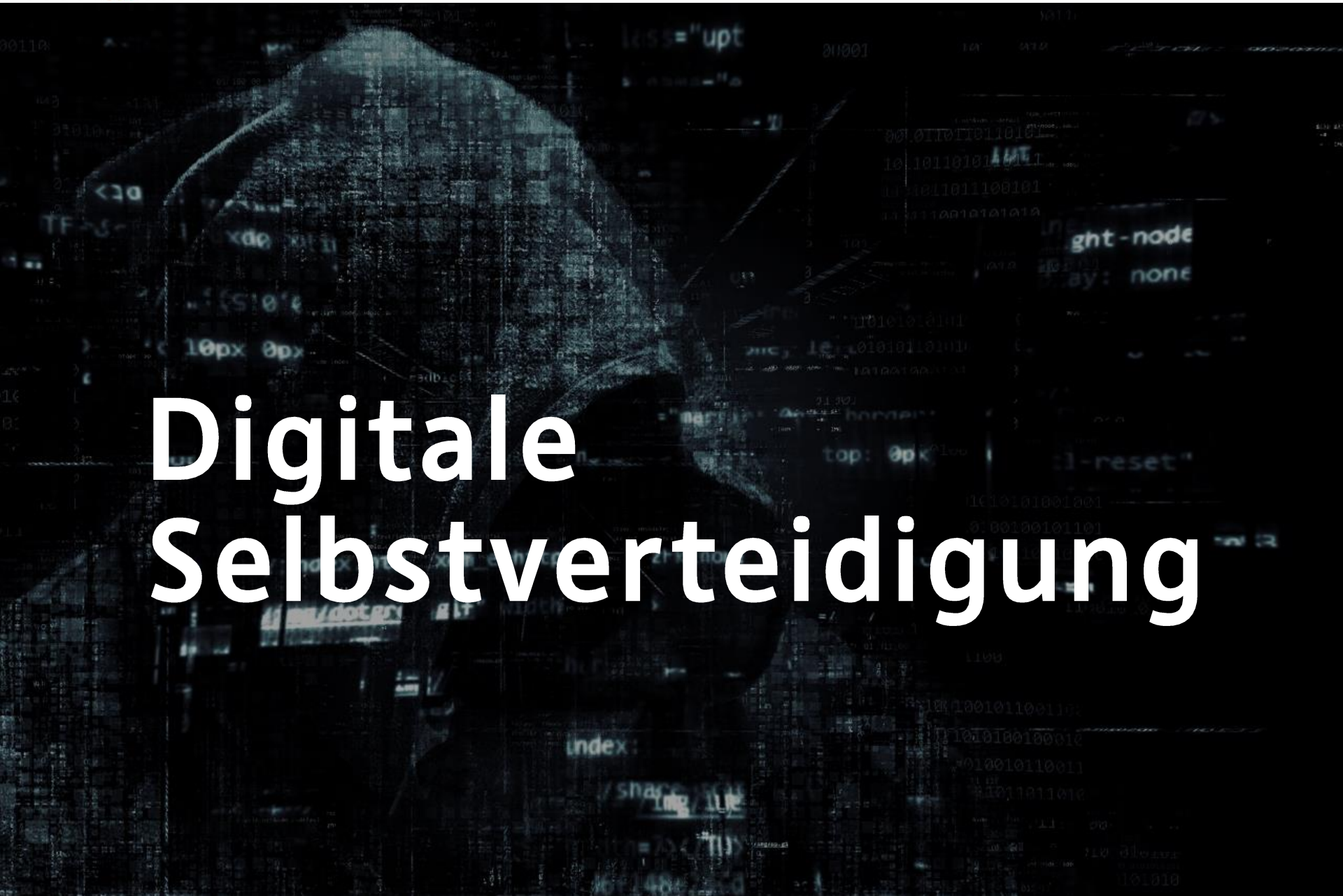

Digitale
Selbstverteidigung

Meine Daten gehören mir.

Nicht erst seit dem NSA-Skandal sind Themen wie Datensammeln, Überwachung und Privatsphäre in den Fokus der Öffentlichkeit gerückt.

Auch der letzte „Datenklau“ von „Prominenten“ und Mitgliedern des Bundestages zeigt, dass unsere Daten dann doch nicht so sicher sind, wie wir das gern glauben wollen.

Umso wichtiger ist es, sich mit einfachen Mitteln dagegen zu schützen.

Wir zeigen Euch, was Ihr selbst dazu beitragen könnt.

Faktor Mensch

Das größte Problem bei der Nutzung von Apps, sozialen Netzwerken, Suchmaschinen und co sitzt immer noch vor dem Computer.

Es ist der MENSCH.
DU. WIR.

Jeder noch so gute Ratschlag wird scheitern, wenn wir ihn nicht anwenden. Jedes noch so gute Tool wird uns nichts helfen, wenn wir es nicht oder falsch benutzen.

Es geht nicht nur um unsere persönlichsten Daten. Sondern auch unserer Privatsphäre und unsere Freiheit.

Erst denken, dann nutzen.

Jeder der sich mit dem Internet verbindet hinterlässt Datenspuren.

Ob gewollt (Einkaufsprozesse im Online-Shop) oder ungewollt (Übersendung alle gespeicherten Telefonnummern an Whatsapp) ... diese Daten werden erhoben, gespeichert und verarbeitet.

Oft genug werden Eure Daten dann auch weiterverkauft.

Das wirksamste Prinzip zum Schutz Eurer Daten ist es, diese nur dann einzugeben, wenn sie wirklich benötigt werden.

Der Grundsatz dabei sollte stets lauten:

„Weniger ist mehr!“

Es besteht absolut keine Notwendigkeit, bei Facebook eine Telefonnummer zu hinterlegen. Selbst wenn Facebook Euch permanent damit nervt.

Eine „smarte“ Zahnbürste braucht weder Zugriff auf Euer Smartphone-Mikrofon, oder gar auf die Kontakte oder Bilder.

Informiert Euch VOR Nutzung von Online-Angeboten oder Apps, was mit Euern Daten geschieht.

Überlegt Euch, ob Ihr das Produkt oder die Dienstleistung wirklich braucht. Oder ob es nicht auch der Offline-Einkauf oder eine normale Zahnbürste tut.

„Passwort1“ … ist großer Mist.

Passwörter begegnen uns an jeder Ecke im Internet.
Sie sind quasi der **Schlüssel** zu unserer virtuellen Wohnungstür.

Und würden wir diesen Schlüssel jedem Fremden einfach so in die Hand drücken oder überlassen? Ganz sicher nicht.

Daher sollten Eure Passwörter nicht nur leicht zu merken, **sondern vor allem sicher sein.**
Der Grundsatz „Weniger ist mehr!“ gilt hier NICHT.

„Passphrasen“ (Eselsbrücken) erleichtern das „Merken“ der Passwörter. Man erstellt sie aus einem beliebigen Satz.
Und sie sind nebenbei meist auch ziemlich sicher.

Ein Passwort sollte mindestens 8 Zeichen umfassen, besser sind 16 oder mehr.
Sehr gut sind dabei 4-5 (zufällige) Worte, die man nahtlos hintereinander schreibt.

Vermeidet Begriffe, die aus normalen Wörterbüchern stammen könnten. Diese sind viel zu leicht zu ermitteln.

Auch bei zu nutzenden Geräten wie dem Router sind meistens voreingestellte Zugangspasswörter vorhanden.
Diese sollten von Euch auch dringend geändert werden.

Geburtsdatum, Namenskombinationen oder der Vorname des Haustiers sind KEINE guten Passwörter. Diese lassen sich mit „Brute-Force“-Methoden leicht auslesen oder ganz einfach schlicht erraten.

Auch wenn es unheimlich bequem ist, ist EIN Passwort für alle Konten/Apps NICHT zu empfehlen. Nutzt für jedes Konto ein anderes Kennwort.
Lasst Euch von Tools wie Keepass dabei helfen.

Passwortmanager/Passphrase

Passwortmanager ?

Natürlich muss man sich für alle mögliche Online-Dienste die einzelnen Passwörter nicht zwingend merken. Oder gar aufschreiben.

Hierzu könnt Ihr Tools benutzen, die das für Euch tun.

Eines dieser Tools ist die OpenSource-Software
„Keepass“

Es speichert verschlüsselt alle Eure Kennwörter/Passphrasen für die verschiedensten Online-Anwendungen.

Das Gute: Um es einzusetzen müsst Ihr Euch nur noch
1 Master-Passwort
merken.

Eine Mini-Anleitung findet Ihr im Anhang.

Was ist eine Passphrase?

Eine Passphrase besteht im Vergleich zu einem Passwort aus einer größeren Anzahl an Zeichen. Durch bilden eines Satzes und die Verwendung der vorkommenden Anfangsbuchstaben und Satzeichen entsteht eine einmalige Kombination.

Satz:
„Ich bin 26 Jahre Fußballtrainer, aber habe auch selbst 15 Jahre gespielt.“
Abgeleitet Passphrase:
„Ib26JF,aha15Jg.“

„Entropisch“ sichere Passwörter.

Diese Passwörter entstehen nicht aus Zeichenfolgen. Sondern aus mindestens 4-5 zufällig aneinandergereihten Worten.

Diese sind noch schwerer zu knacken.

Warum genau zeigen wir Euch auf der nächsten Seite.

Passwörter und … Entropie ?

Ok, wir ersparen Euch jetzt einen total nerdigen Vortrag, wie sich diese „Entropie“ berechnet.

Wichtig zu wissen ist allerdings:
Je stärker die Entropie eines Passworts, desto schwieriger ist es zu knacken.

Es müssen nicht immer Passphrasen oder kryptische Zeichen sein.
Mindestens 4-5 zufällig gewählte Wörter, die nahtlos aneinandergereiht werden, können eine sehr hohe Entropie aufweisen.

Beispiel:

„dieschulefaelltwegenbodennebelaus“
(33 Zeichen, 155 bit Entropie))

Hat eine höhere Entropie als

„ l.26Jh!15J“
(10 Zeichen, 65 Bit Entropie)

Oder gar als

„Password1“
(9 Zeichen, 55 Bit Entropie)

Mit **Entropie** bezeichnet man den Informationsgehalt. Also vereinfacht die Anzahl Bits die mindestens gebraucht werden, um die Information einer Nachrichtenquelle darzustellen.

Die Entropie gibt also hinsichtlich der Passwörter an, welchen Aufwand man im Durchschnitt treiben muss, um dieses zu “knacken”.

Alles unter 70 Bit Entropie ist mit der heutigen Generation von leistungsstarken Rechnern oder Grafikkarten innerhalb weniger Stunden bzw. maximal Tagen zu knacken.

Updates, Updates, Updates ...

Ganz egal ob Ihr jetzt via normalem Rechner das Internet nutzt, oder ob Ihr das mit dem Tablet bzw. Smartphone nutzt.

Auf all diesen Geräten ist in der Regel ein Betriebssystem vorinstalliert.

Egal ob Windows, Linux, Mac-OS (Rechner/Laptops) oder Android, iOS, WindowsMobile (Smartphone/Tablet):

Keines dieser Systeme ist per se sicher. Weder bei der erstmaligen Benutzung oder im Laufenden Betrieb.

Umso wichtiger ist es, dass Ihr System- bzw. Sicherheitsupdates immer sofort einspielt.

Ja, es ist lästig - aber es schützt auch Eure Daten, wenn Einfallstore für Hacker geschlossen werden.

Wichtige Updates bzw. Sicherheitsupdates verschieben oder nicht zu installieren gefährdet Eure Sicherheit, und damit Eure Daten!

Updates gibt es nicht nur für Betriebssysteme. Auch Software und Apps sollten IMMER auf dem aktuellen Stand gehalten werden.

Updates IMMER nur von der Herstellerseite oder von vertrauenswürdigen Quellen installieren. Prüft also vorher, ob es sich nicht um eine dubiose Quelle/Link handelt.

Erinnerung:
Im Mai 2017 wurde „WannaCry“ bekannt. Kriminelle drangen durch bekannte Sicherheitslücken in Windows in tausende Computer ein und versuchten Lösegelder zu erpressen.

Backup - Notfallsicherung

Nichts ist so langlebig, stabil und sicher, dass es nicht doch irgendwann kaputt geht.
Oder verloren geht.
Oder gehackt wurde.

Natürlich ist der Frust dann groß, wenn ohne Vorwarnung alle wichtigen gespeicherten Daten mit einem Mal weg sind.

Daher sollte jeder von seinen Daten, egal ob auf Rechner oder Smartphone, **regelmäßige Sicherheitskopien** (Backups) anlegen.

Ihr könnte dazu natürlich auch Cloud-Speicher großer Anbieter nutzen.

Wir **empfehlen** jedoch, diese Daten auf einer **separaten Festplatte zu sichern**, die nicht mit dem Internet verbunden ist.

Damit sind diese weder durch Hacker angreifbar, noch können Daten dann durch Dritte ausgelesen bzw. verwendet werden.

Ein Backup ist keine einmalige Sache. Sichert Eure Daten regelmäßig. Mindestens einmal im Monat sollte Euch der Schutz Eurer Daten das Wert sein.

Ein Backup sollte nie auf dem gleichen Medium liegen, wie die Originaldateien. Auch Partitionen auf der gleichen Festplatte sind strikt zu meiden. Festplatte kaputt = alle Daten weg.

Achtet darauf, dass Ihr beim Backup die Daten auch verschlüsselt übertragt (bei Nutzung Cloud) bzw. ablegt. Nur dann sind sie wirklich sicher.

Kostenlose OpenSource-Backup-Tools können Euch helfen, diese wichtige Arbeit zu automatisieren.
Hier gehts zu einer Liste mit OpenSource-Tools

Für regelmäßige Backups reichen auf normalen Rechnern die mitgelieferten Systemtools völlig aus.

E-Mail - Verschlüsselung

Es gibt ja kaum einen Dienst, bei dem man nicht auf eine Maildresse angewiesen ist.
Ob es nur zur Anmeldung, Verifizierung oder Rücksetzung von Passwörtern ist.

Selbst ein Smartphone kann man ohne Mailadresse kaum benutzen.

Es stehen also mitunter auch viele persönliche Daten in einer solchen Mails.

Dabei muss Euch klar sein, dass eine unverschlüsselte Mail wie eine normale Postkarte ist.
JEDER kann sie lesen.

Wenn Ihr wollt das genau das nicht passiert, müsst Ihr Eure Mail **verschlüsseln**.

Und keine Angst, es klingt komplizierter als es ist.

Nutzt statt des Webmailers ein eigenes Mailprogramm. OpenSource-Software wie „Thunderbird“ hat alle notwendigen Funktionen und lässt sich erweitern.

Kostenlose Tools wie „Enigmail“ für Thunderbird oder „4GPWIN“ für Outlook helfen Euch Mails zu verschlüsseln.

Eine Anleitung für das Verschlüssen von Mails findet Ihr im Anhang..

Nutzt die von Piraten vor Ort angebotenen „Crypto-Partys“. Hier wird Euch Schritt-für-Schritt“ auch die Verschlüsselung erläutert

E-Mail – Phishing und Co

Die meisten Angriffe auf höchst sensible Daten wie Bankverbindung, Log-In-Daten, Passwörter und Co erfolgen durch sogenanntes **„Phishing“.**

Hier versuchen Kriminelle über gefälschte Webseiten und E-Mails an Eure persönliche Daten zu gelangen und damit Identitätsdiebstahl zu begehen.

Schützt Euch selbst, in dem Ihr beispielsweise das die Online-Banking-Seite NIEMALS über einen Link in einer Mail aufruft. Tippt die Webadresse Eurer Bank von Hand in den Browser ein.

Prüft immer den Absender der Mail. Selbst wenn das als Name „Sparkasse x“ steht, kann diese von einem Kriminellem kommen.

Wenn Ihr unsicher seid, schaut Euch immer den gesamten „Header“ der Mail an. Meistens wird hier der Betrug schnell erkennbar.

Beigefügte Dateianlagen von unbekannten Absenden niemals öffnen. Auch in diesen können sich trojanische Pferde verstecken.

Links, die Euch zum Anmelden an Webseiten oder Freischalten von Konten auffordern, niemals direkt aus der Mail heraus öffnen. Kopiert diese in den Browser und schaut Euch die Webseite vorher genau an.

Nutzt die von Piraten vor Ort angebotenen „Crypto-Partys“. Hier wird Euch Schritt-für-Schritt“ auch der Umgang mit Phishing-Mails erläutert.

Messenger und Co

Ein Großteil der Kommunikation läuft heute über das Smartphone, und da über Messenger-Dienste.

Die meisten von Euch werden Whatsapp nutzen. Klar, es ist bequem, mit vielen Funktionen ausgestattet und fast jeder hat es.

Doch trotz aller Versprechungen des Anbieters Eure Privatsphäre zu schützen, sind Eure Daten trotz Verschlüsselung nicht sicher.

Euer gesamtes Adressbuch inkl. Aller Telefonnummern wird ohne Rückfrage an die Server übertragen.

Facebook, zu dem Whatsapp gehört, verwendet auch all Eure gesendeten Meta-Daten und kommerzialisiert diese.

Nutzt daher alternative Messenger, die Eure Privatsphäre wirklich ernst nehmen.

Sichere Alternativen zu Whatsapp:

- Signal
- Threema
- Telegram

Telegram und Threema lassen sich auch komplett OHNE Telefonnummer nutzen

Alternativ lässt sich auch der XMPP-Standard nutzen. Dieser ist auch als „Jabber“ bekannt und erfüllt ebenso alle wichtigen Anforderungen.

Nutzt die von Piraten vor Ort angebotenen „Crypto-Partys“. Hier wird Euch Schritt-für-Schritt“ auch der Umgang mit Phishing-Mails erläutert.

Anonym Surfen?

Bei jedem Besuch im Web geben Sie eine Menge persönlicher Informationen preis, ohne es zu wissen.

Neben der aktuellen IP-Adresse werden unter anderem auch die Windows-Version und verwendeter Webbrowser samt Plug-ins übermittelt. Diese Infos könnten bösartige Angreifer verwenden, um sich bekannte Sicherheitslücken (Exploits) zunutze zu machen und in ein fremdes System einzubrechen.

Doch auch die Werbeindustrie interessiert sich für Ihr Surfverhalten.

Anonymes Surfen schützt Eure Privatsphäre!

Und geht einfacher als gedacht.

Nutzt die von Piraten vor Ort angebotenen „Crypto-Partys“. Hier wird Euch Schritt-für-Schritt“ auch der Umgang mit „TOR“ erläutert.

Surfen via „VPN“

Vereinfacht ausgedrückt handelt es sich dabei um eine Software, die über eine als Tunnel bezeichnete, verschlüsselte Verbindung den Kontakt zu einem Remote-Server herstellt, sodass der eigene Rechner Teil dieses Netzwerks wird, und fortan mit dessen IP-Adresse im Internet unterwegs ist.

Nachteil: Gute Services kosten Geld.

Surfen via „TOR-Browser“

Während des Surfens im Browser werden die Daten verschlüsselt an einen Tor-Server übermittelt. Dieser leitet es an einen anderen weiter, der die Daten ebenfalls weitergibt – in der Regel sind es drei Stationen. Welche Route das Datenpaket dabei einschlägt, wird vom Onion-Proxy zufällig bestimmt. Eure IP ist dabei NICHT mehr rückverfolgbar.

Vorteil: „Kost nix“ und mehr Anonymität im Web geht nicht.

Nachteil: Mitunter etwas langsamer als Firefox und Co.

Suchmaschinen

Wer im Internet irgendetwas sucht, der „googelt“.

Google hat es mit seiner Suchmaschine sogar in den Duden geschafft. „Googeln“ als Begriff kennt wohl jeder von Euch.

Aber wusste Ihr auch, dass Google einerseits während des Suchens

- jede Menge persönliche Daten von Euch sammelt, speichert und dann kommerzialisiert?
- Suchergebnisse nicht ganz so objektiv sind, wie Google das behauptet ?

Das muss nicht sein.

Es gibt auch zu Google sinnvolle und datensparsame Alternativen, die Eure Privatsphäre respektieren.

Alternativen zu Google, Bing und Co.

Startpage.com

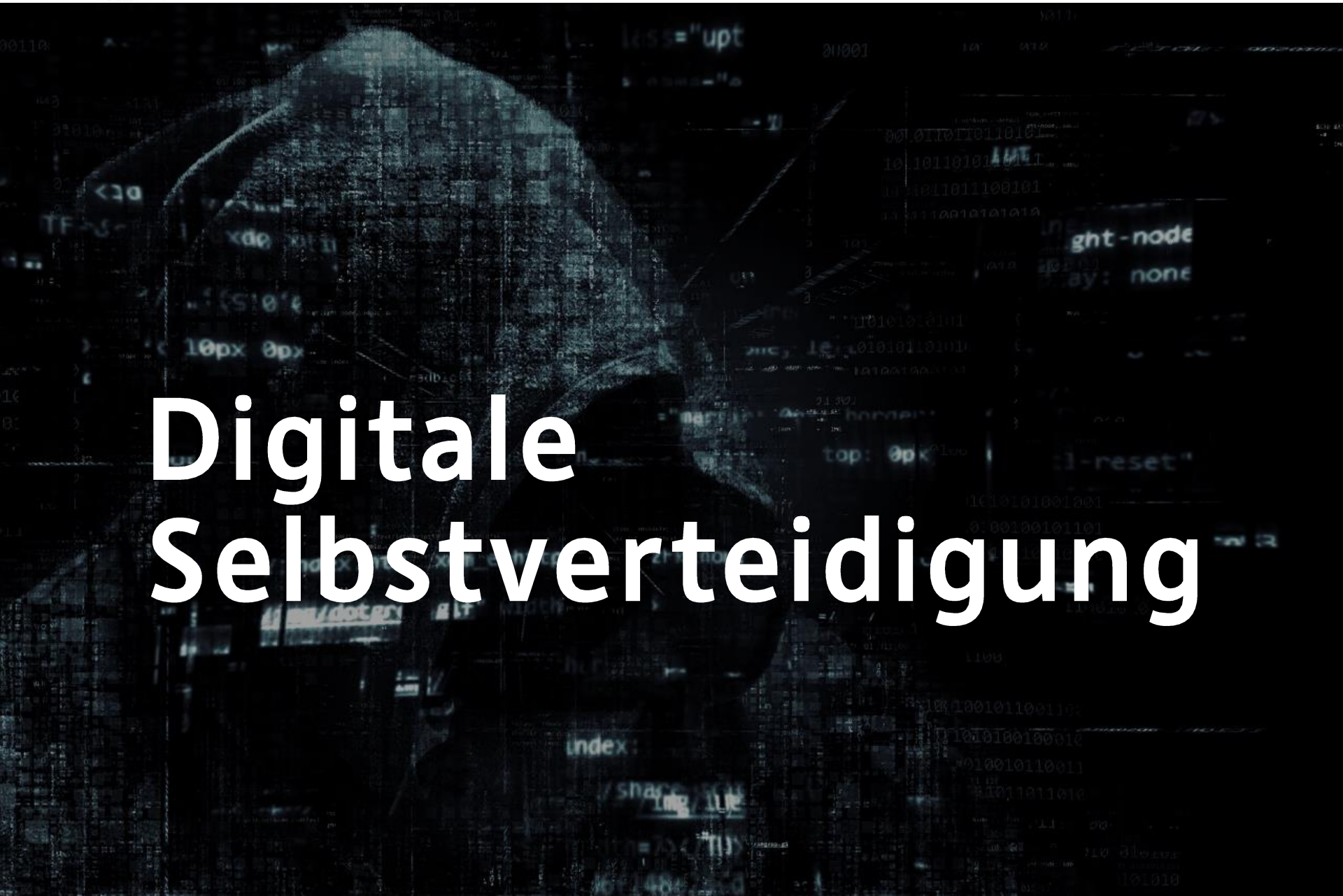
Die niederländliche Seite nutzt zwar den Google-Suchindex, übermittelt aber keine persönlichen Daten.

Metager.de

Sehr datenschutzfreundliches Open-Source Angebot aus Deutschland. Keine Speicherung oder Übertragung persönlicher Daten. Nutzt anonymen Proxy und TOR-hidden-Zugang.

Duckduck.go

Speichert keine nutzerbezogenen Daten (Surfverhalten).
Nutzt aber AWS und unterliegt damit genau wie Google dem „Patriot act“. Amerikanische Geheimdienste können somit Daten verlangen.


Digitale
Selbstverteidigung