Internet

Intranet

Darknet

Überblick und Einordnung

Quellenangabe in den Textabschnitten.

Surface Web (Internet, offenes Netz, **dort, wo wir uns meistens bewegen**)

Deep Web (Zugang nur durch Zulassungen)

Darknet (anonym, legal und illegal)

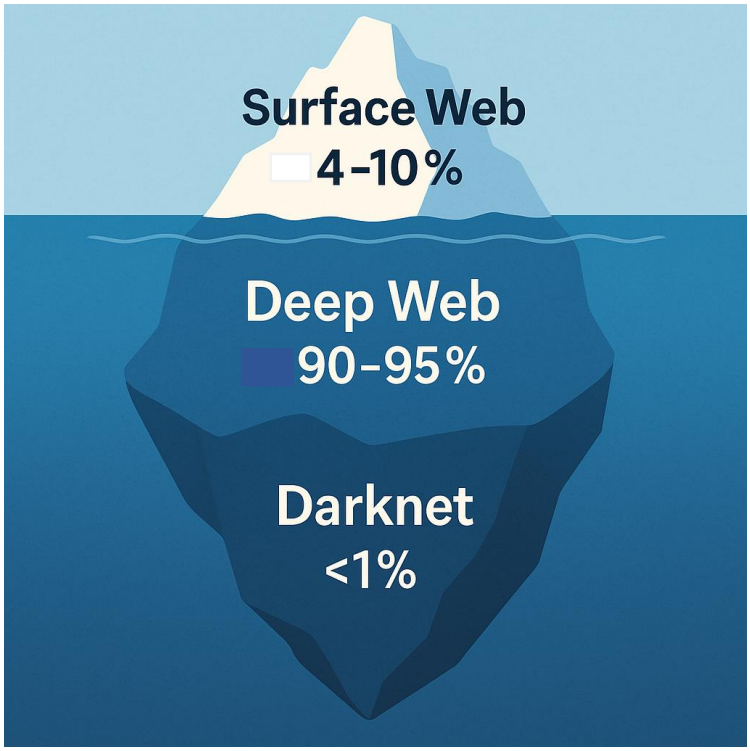

Abbildung 1 KI-Grafik

1. **Das Surface (Clear) Web:** Das ist der Bereich des Internets, in dem wir surfen, shoppen, mit Freunden chatten oder Urlaubsfotos hochladen. Dieser leicht zugängliche Teil des Internets ist jedoch nur ein kleines Fragment des gesamten Netzes.
2. **Das Deep Web:** In diesem mit Abstand umfangreichsten Bereich (ca. 90% des gesamten Internets) befinden sich Firmendatenbanken, Streaming-Server sowie Online-Speicher (z.B. Cloud-Speicher). Grundsätzlich steht das Deep Web allen offen, viele Inhalte sind jedoch geschützt, um bspw. Unternehmensgeheimnisse zu schützen.
3. **Das Darknet:** Dieser Raum des Internets ist ein vergleichsweise kleines Teilstück des Deep Webs. Es ist nicht auf herkömmliche Weise auffindbar, die Kommunikation wird verschlüsselt und die Urheberinnen und Urheber der Inhalte sowie seine Besucherinnen und Besucher bzw. die Konsumentinnen und Konsumenten wollen möglichst anonym bleiben.

Quelle: *Bundesamt für Sicherheit in der Informationstechnik*

Unterschiede zwischen Internet, Intranet und Darknet

1. Internet (Das offene Web, Oberflächennetz) ***Hier bewegen wir uns normalerweise als Nutzer.***

* Definition: Das globale System von miteinander verbundenen Computernetzwerken, das die standardisierte Internetprotokollfamilie (TCP/IP) verwendet, um Milliarden von Nutzern weltweit zu bedienen. Es ist öffentlich zugänglich.

* Zugang: Für jeden mit einer Internetverbindung und einem Standard-Webbrowser (wie Chrome, Firefox, Safari) zugänglich. Informationen werden in der Regel von Suchmaschinen wie Google und Bing indiziert und sind somit leicht auffindbar.

* Inhalt: Enthält eine riesige Menge an öffentlich verfügbaren Informationen, Websites, Diensten und Anwendungen für Kommunikation, Handel, Unterhaltung, Bildung und mehr.

* Sicherheit: Im Allgemeinen offen und weniger sicher als private Netzwerke. Die Sicherheit beruht auf Protokollen wie HTTPS, Firewalls und dem Bewusstsein der Nutzer.

* Anteile am Gesamtnetz: Das offene Web wird Schätzungen zufolge nur einen relativ kleinen Teil des gesamten digitalen Inhalts ausmachen, oft zwischen 4-10%.

2. Intranet (Teil vom Deep Web)

* Definition: Ein privates Netzwerk, das innerhalb einer Organisation betrieben wird. Es verwendet Internetprotokolle, Netzwerkverbindungen und oft die gleichen Technologien wie das öffentliche Internet, ist aber nur für autorisierte Benutzer innerhalb dieser Organisation zugänglich (z. B. Mitarbeiter eines Unternehmens).

* Zugang: Erfordert eine Authentifizierung (wie Benutzername und Passwort) für den Zugriff. Es befindet sich typischerweise hinter einer Firewall und ist für die breite Öffentlichkeit nicht zugänglich. Informationen werden in der Regel nicht von öffentlichen Suchmaschinen indexiert.

* Inhalt: Enthält interne Unternehmensinformationen, Dokumente, Anwendungen, Kommunikationstools und Ressourcen, die zur Erleichterung interner Arbeitsabläufe, Zusammenarbeit und Kommunikation entwickelt wurden.

* Sicherheit: Sicherer als das öffentliche Internet aufgrund des eingeschränkten Zugriffs und der internen Kontrolle.

* Anteile am Gesamtnetz: Es ist schwierig, den genauen prozentualen Anteil des gesamten Netzwerks zu quantifizieren, den Intranets ausmachen. Sie existieren als private Netzwerke und ihre Daten werden nicht öffentlich indexiert. Angesichts der großen Anzahl von Organisationen weltweit ist die Gesamtmenge der Daten in Intranets jedoch wahrscheinlich beträchtlich.

3. Darknet oder Dark Web (Teil vom Deep Web)

* Definition: Ein bewusst versteckter Teil des Internets, der nicht von Standard-Suchmaschinen indexiert wird und spezielle Software, Konfigurationen oder Autorisierungen für den Zugriff erfordert. Es existiert innerhalb des Deep Webs.

* Zugang: Erfordert spezielle Software wie Tor (The Onion Router), um darauf zuzugreifen. Websites im Darknet verwenden verschleierte Adressen (wie ".onion"-Adressen für Tor) und sind über reguläre Browser nicht auffindbar.

* Inhalt: Enthält sowohl legale als auch illegale Inhalte. Es ist bekannt dafür, Anonymität zu bieten, die für illegale Aktivitäten wie illegale Marktplätze, aber auch für legitime Zwecke wie sichere Kommunikation für Whistleblower und Aktivisten genutzt werden kann.

* Sicherheit: Bietet ein höheres Maß an Anonymität und Privatsphäre im Vergleich zum Oberflächennetz, was es aber nicht per se sicher macht. Nutzer können weiterhin anfällig sein.

* Anteile am Gesamtnetz: Das Darknet ist ein sehr kleiner Bruchteil des gesamten Internets. Schätzungen deuten darauf hin, dass es etwa 0,01% bis 5% des Deep Webs ausmacht, welches selbst etwa 90-96% des gesamten Internets umfasst.

Zusammenfassung:

Zuordnung	Surface Web (Oberflächennetz)	Deep Web	Deep Web
Merkmale	Internet (Clear Web)	Intranet	Darknet
Zugang	Für alle mit Internetanschluss, öffentlich zugänglich	Nicht öffentlich zugänglich, auf Organisationen beschränkt	Erfordert spezielle Software
Indexierung (Erklärung weiter unten)	Von Suchmaschinen indexiert	In der Regel nicht indexiert	Bewusst nicht indexiert
Inhalt	Öffentliche Informationen, Dienste, Webseiten, alles was Google & Co finden können, Ausnahmen: Online-Banking, Emails etc. nur mit PW und über sichere Verbindungen und nicht indexiert	Firmen interne Portale, Datenbanken, passwortgeschützte Bereiche, Behörden, Universitäten, Streaming-Server, Cloud-Speicher etc.	Anonyme Kommunikation, sowohl legal als auch illegal, Marktplätze, Foren
Sicherheit	Relativ offen	Sicher durch Beschränkungen	Zielt auf Anonymität ab, Sicherheit variiert
Größe (Web-Inhalte)	4-10%	90-96%	0,01-5%
Teil von	World Wide Web	Privaten Netzwerken unter Nutzung von Netzwerktechnologie	Versteckter Teil des Deep Webs

Das Darknet, eine Positionierung.

Wie es der Name schon andeutet, ist das Darknet ein dunkles, also verborgenes Netzwerk. Dabei ist es nicht getrennt vom sichtbaren Internet, dem Clear Web, sondern hängt mit diesem zusammen. Grundsätzlich sollte man wissen, dass das gesamte Internet aus drei wesentlichen Komponenten besteht:

4. **Das Clear Web:** Das ist der Bereich des Internets, in dem wir surfen, shoppen, mit Freunden chatten oder Urlaubsfotos hochladen. Dieser leicht zugängliche Teil des Internets ist jedoch nur ein kleines Fragment des gesamten Netzes.
5. **Das Deep Web:** In diesem mit Abstand umfangreichsten Bereich (ca. 90% des gesamten Internets) befinden sich Firmendatenbanken, Streaming-Server sowie Online-Speicher (z.B. Cloud-Speicher). Grundsätzlich steht das Deep Web allen offen, viele Inhalte sind jedoch geschützt, um bspw. Unternehmensgeheimnisse zu schützen.
6. **Das Darknet:** Dieser Raum des Internets ist ein vergleichsweise kleines Teilstück des Deep Webs. Es ist nicht auf herkömmliche Weise auffindbar, die Kommunikation wird verschlüsselt und die Urheberinnen und Urheber der Inhalte sowie seine Besucherinnen und Besucher bzw. die Konsumentinnen und Konsumenten wollen möglichst anonym bleiben.

   Quelle: *Bundesamt für Sicherheit in der Informationstechnik*

Der Hauptunterschied zwischen dem regelbasierten Internet (auch bekannt als Clearnet) und dem Darknet liegt in
dem Zugang, der Anonymität und der Art der Inhalte.

Clearnet (Surface Web, Oberflächennetz)

Zugang:

- **Das Clearnet ist der Teil des Internets, den wir täglich nutzen.** Es ist über Standard-Webbrowser wie Chrome, Firefox oder Safari zugänglich.
- Websites und Inhalte sind indexiert. Somit wird Suchmaschinen wie Google, DuckDuckGo, Startpage usw. ermöglicht, das riesige und ständig wachsende Netz von Webseiten zu organisieren, durchsuchbar zu machen und Inhalte leicht aufzufinden. (Detaillierte Beschreibung zur Indexierung weiter unten im Text).

Anonymität:

- Die Aktivitäten im Clearnet sind in der Regel nachverfolgbar. IP-Adressen und andere Daten können verwendet werden, um Benutzer zu identifizieren.
- Die Privatsphäre ist oft eingeschränkt, da viele Websites und Dienste Benutzerdaten sammeln.

Inhalte:

- Das Clearnet enthält eine breite Palette von Inhalten, von Nachrichten und sozialen Medien bis hin zu E-Commerce und Online-Diensten.
- Es unterliegt Gesetzen und Vorschriften, die illegale Aktivitäten einschränken.

Darknet

Zugang:

- **Das Darknet ist ein Teil des Internets, der spezielle Software, Konfigurationen und Autorisierungen erfordert, um darauf zuzugreifen.**
- Es ist nicht über Standard-Webbrowser zugänglich. Hier kommen der Browser Tor und das TOR-Netzwerk zum Einsatz. Siehe eigenen Aufsatz zum Browser TOR (The Onion Router).
- Darknetseiten sind nicht von Suchmaschinen wie Google, DuckDuckGo usw. indexiert.

Anonymität:

- Das Darknet bietet ein höheres Maß an Anonymität, da die Identität der Benutzer und der Standort von Websites verschleiert werden.
- Dies wird durch Verschlüsselung und die Weiterleitung des Datenverkehrs über mehrere Server erreicht.

Inhalte:

- Das Darknet beherbergt eine Vielzahl von Inhalten, darunter **sowohl legale als auch illegale Aktivitäten.**
- Es kann für den Austausch sensibler Informationen, den Schutz der Privatsphäre oder die Umgehung von Zensur verwendet werden.
- Es ist jedoch auch bekannt für illegale Märkte, auf denen Drogen, Waffen und gestohlene Daten gehandelt werden.

Zusammenfassend:

> Das Clearnet ist öffentlich zugänglich und indexiert, während das Darknet verborgen und anonym ist.
> Das Clearnet ist reguliert und enthält eine breite Palette von Inhalten, während das Darknet ein höheres Risiko für illegale Aktivitäten birgt.

Die Indexierung im Internet ist ein entscheidender Prozess, der es Suchmaschinen wie Google, DuckDuckGo, Startpage u.a. ermöglicht, das riesige und ständig wachsende Netz von Webseiten zu organisieren und durchsuchbar zu machen.

Generell:

- Indexierung ist der Prozess, bei dem Suchmaschinen Informationen von Webseiten sammeln, analysieren und in ihren riesigen Datenbanken (den sogenannten Indizes) speichern.
- Dieser Index ist wie ein riesiges Inhaltsverzeichnis des Internets, das Suchmaschinen hilft, relevante Ergebnisse für Suchanfragen schnell zu finden.

Funktion:

- Suchmaschinen verwenden sogenannte „Crawler“ oder „Bots“, um das Internet zu durchsuchen. Diese Bots folgen Links von Webseite zu Webseite und sammeln dabei Informationen über den Inhalt jeder Seite.
- Die gesammelten Informationen werden analysiert und nach verschiedenen Kriterien wie Inhalt, Keywords, Struktur und Links geordnet.
- Diese Informationen werden dann im Index der Suchmaschine gespeichert, wo sie für Suchanfragen zur Verfügung stehen.
- Der Index wird ständig aktualisiert, um neue Webseiten und Änderungen an bestehenden Webseiten zu berücksichtigen.

Ranking:

- Wenn ein Nutzer eine Suchanfrage eingibt, durchsucht die Suchmaschine ihren Index nach relevanten Ergebnissen.
- Algorithmen bestimmen die Reihenfolge der Suchergebnisse (das Ranking) basierend auf verschiedenen Faktoren wie Relevanz, Qualität und Popularität.

Bedeutung der Indexierung

- Die Indexierung ist entscheidend für die Funktionsweise von Suchmaschinen. Ohne sie wäre es unmöglich, relevante Informationen im Internet zu finden.
- Für Webseitenbetreiber ist die Indexierung wichtig, um sicherzustellen, dass ihre Webseiten in den Suchergebnissen erscheinen.
- Die Indexierung ist auch wichtig für die Suchmaschinenoptimierung (SEO). Durch SEO kann man die Wahrscheinlichkeit erhöhen das eine Webseite im Index der Suchmaschine gelistet wird.

Wer in die (zum Teil gefährliche) Darknet-Welt Zugang benötigt, findet hier eine kurze Anleitung:

Beachte, der Zugriff auf das Darknet erfordert spezielle Software, Konfigurationen und Kenntnisse. Hier ist eine grundlegende Anleitung, aber beachte, dass der Zugriff auf das Darknet Risiken birgt und illegale Aktivitäten strafrechtliche Konsequenzen haben können:

1. Tor Browser herunterladen und installieren:
 - Der Tor Browser ist die am häufigsten verwendete Software für den Zugriff auf das Darknet. Er ist kostenlos und kann von der offiziellen Tor Project Website heruntergeladen werden.
 - Stelle sicher, dass du den Browser von der offiziellen Website herunterlädst, um gefälschte Versionen zu vermeiden.
 - Installiere den Tor Browser wie jede andere Software.
2. Tor Browser konfigurieren:
 - Nach der Installation öffne den Tor Browser.
 - Der Browser verbindet sich automatisch mit dem Tor-Netzwerk. Dies kann einige Zeit dauern.
 - Es wird empfohlen, die Sicherheitseinstellungen des Browsers nicht zu ändern, da dies die Anonymität beeinträchtigen könnte.
3. Auf Darknet-Websites zugreifen:
 - Darknet-Websites haben spezielle Adressen, die als **".onion"-Adressen** bezeichnet werden. Diese Adressen können nicht in normalen Browsern aufgerufen werden.
 - Um Darknet-Websites zu finden, kannst du **Suchmaschinen wie Ahmia oder OnionLand** Search verwenden.
 - Es gibt auch sogenannte Linklisten, die eine Zusammenstellung von .onion Seiten beinhalten.
 - **Sei vorsichtig beim Anklicken von Links im Darknet, da viele Websites illegal oder schädlich sein können.**

Wichtige Sicherheitshinweise:

 - *Verwende immer ein VPN in Kombination mit dem Tor Browser, um deine Anonymität zu erhöhen.*
 - *Niemals JavaScript im Tor Browser aktivieren, da dies deine Anonymität gefährden kann.*
 - *Gib niemals persönliche Informationen im Darknet preis.*
 - *Lade keine Dateien aus dem Darknet herunter, da sie Viren oder Malware enthalten könnten.*
 - *Sei dir der Risiken bewusst, bevor du auf das Darknet zugreifst.*

Zusätzliche Informationen:

1. Das Darknet ist nicht illegal, aber es wird häufig für illegale Aktivitäten genutzt.
2. Der Zugriff auf bestimmte Inhalte im Darknet kann illegal sein.
3. Sei vorsichtig und informiere dich gründlich, bevor du auf das Darknet zugreifst.

Das Tor Netzwerk funktioniert nach eigenen Regeln.

Unbedingt beachten, man kann es nicht oft genug erwähnen!:

- Niemals echte Daten eingeben (Name, Mailadresse, Kreditkarten etc.)
- Keine Dateien herunterladen, wenn du der Quelle nicht absolut vertraust.
- Skripte im Tor Browser deaktivieren (sind meist schon standardmäßig blockiert).
- Kein JavaScript, keine Plugins, kein Torrent → alles kann deine IP verraten.
- Nie im Vollbildmodus surfen (das kann zur Wiedererkennung führen).
- Kein Login bei Diensten wie Google, Amazon etc. – sonst ist die Anonymität dahin.
- Legale Nutzung ist natürlich entscheidend – manche Inhalte/Marktplätze im Darknet sind illegal. Reine Neugier ist okay, aber vorsichtiger Umgang ist Pflicht.

. onion-Adressen aufrufen
Statt https://... verwendet man z. B. http://xxxxxxxxxxxx.onion. Diese Adressen findest du nicht bei Google, sondern auf spezialisierten Verzeichnisseiten. (Vorsicht bei dubiosen Links!).

Alle Links funktionieren nur im Tor Browser. .onion-Adressen sehen oft „komisch“ aus – das ist normal. Seiten können langsam laden, da Tor-Verbindungen umgeleitet werden.

Hier ist eine seriöse und legale Liste von .onion-Webseiten, die man mit dem Tor Browser aufrufen könnte. Diese Angebote stammen von etablierten Medien, Menschenrechts-organisationen und sicheren Diensten. **Links wurden verändert und unbenutzbar gemacht.:**

1. ProPublica (investigativer Journalismus, USA)
Adresse: http://www.propubespa33w.onion/

2. Deutsche Welle (DW – deutschsprachige Nachrichten)
Adresse: http://dwnewsviamwnp.onion/

3. BBC News (britische Nachrichten)
Adresse: http://bbcnewsvtpsuy.onion/

4. The New York Times (US-Nachrichten)
Adresse: http://nytimesfgragh.onion/

5. Riseup (sicherer E-Mail- & VPN-Dienst für Aktivist:innen)
Adresse: http://7qbl3dyi3jmiy.onion/

6. SecureDrop (anonymes Whistleblower-Tool, z. B. für Medienhäuser)
Viele Redaktionen haben eigene SecureDrop-Adressen, z. B.:
Spiegel: http://v6pua3i5fq76p.onion/
Guardian: http://33y6fjyphzfjj.onion/
Washington Post: http://jcw5q6uyjpxcc.onion/

Quelle für den folgenden Aufsatz: *Bundesamt für Sicherheit in der Informationstechnik*

Der verborgene Teil des Internets, den man im Allgemeinen Darknet nennt, sei ein Tummelplatz für kriminelle Machenschaften, heißt es. Und fast jeder hat schon Geschichten gehört, nach denen im Darknet Drogen, Waffen, Menschen oder sogar Morde gehandelt werden.

Wie es der Name schon andeutet, ist das Darknet ein dunkles, also verborgenes Netzwerk. Dabei ist es nicht getrennt vom sichtbaren Internet, dem Clear Web, sondern hängt mit diesem zusammen. Grundsätzlich sollte man wissen, dass das gesamte Internet aus drei wesentlichen Komponenten besteht:

1. **Das Clear Web:** Das ist der Bereich des Internets, in dem wir surfen, shoppen, mit Freunden chatten oder Urlaubsfotos hochladen. Dieser leicht zugängliche Teil des Internets ist jedoch nur ein kleines Fragment des gesamten Netzes.
2. **Das Deep Web:** In diesem mit Abstand umfangreichsten Bereich (ca. 90% des gesamten Internets) befinden sich Firmendatenbanken, Streaming-Server sowie Online-Speicher (z.B. Cloud-Speicher). Grundsätzlich steht das Deep Web allen offen, viele Inhalte sind jedoch geschützt, um bspw. Unternehmensgeheimnisse zu schützen.
3. **Das Darknet:** Dieser Raum des Internets ist ein vergleichsweise kleines Teilstück des Deep Webs. Es ist nicht auf herkömmliche Weise auffindbar, die Kommunikation wird verschlüsselt und die Urheberinnen und Urheber der Inhalte sowie seine Besucherinnen und Besucher bzw. die Konsumentinnen und Konsumenten wollen möglichst anonym bleiben.

Darknet und Tor-Netzwerk

Webseiten des Darknets sind nicht durch die üblichen Suchmaschinen oder Browser auffindbar. Nur mit Hilfe von Anonymisierungsnetzwerken wie Tor ("The Onion Router") sind Seiten im Darknet entweder direkt oder über Darknet-Suchmaschinen abrufbar. Die Seiten sind demnach meist nur direkt (Peer-to-Peer) aufrufbar und nur wenn man die genaue URL kennt.

Das Tor-Netzwerk ist - der namentlichen Ableitung nach - wie eine Zwiebel aufgebaut und verschleiert durch mehrere verschlüsselte Weiterleitungen zwischen den Servern bis hin zum Exit-Node bzw. der entsprechenden Seite im Darknet die Identität der Nutzerinnen und Nutzer. Dabei kennt jeder Knotenpunkt nur jeweils den vorherigen sowie den folgenden Server. Eines sei jedoch klar gesagt: Trotz der Verwendung von Anonymisierungsnetzwerken wie Tor kann eine Zurückverfolgung nicht ausgeschlossen werden.

Quelle: *Bundesamt für Sicherheit in der Informationstechnik*

Darknet und Deep Web – wo liegen die Unterschiede?

Das Deep Web macht etwa 90% des gesamten World Wide Web aus. Seiten des Deep Web sind nicht indexiert und somit nicht über Suchmaschinen erreichbar. Das Deep Web besteht aus Datenbanken, Webseiten und Services, die zu Unternehmen, Behörden oder Universitäten gehören. Diese Inhalte sind meist zahlungspflichtig, vertraulich oder beispielsweise passwortgeschützt, aber harmlos, d.h. nicht illegal oder kriminell.
Für das Darknet braucht man hingegen spezielle Software und seine Inhalte haben häufiger kriminellen Hintergrund.

Ist das Darknet Tummelplatz für Kriminelle?

Einerseits ist das Darknet tatsächlich ein Handelsplatz für Straftaten und illegale Güter aller Art, bei dem die Angebote meist mit sogenannten Kryptowährungen bezahlt werden. Kriminelle nutzen hierfür die verschlüsselte Kommunikation und die damit einhergehende Anonymität des Netzes. Hier liegen auch die größten Gefahren des Darknets: Das Risiko der Verbreitung von Schadsoftware ist hier höher als im Clear Web. Besucherinnen und Besucher können hier auf dubiose Angebote innerhalb des Darknets hereinfallen und sich so entweder strafbar machen oder mit kriminellen Organisationen in Kontakt geraten.

Andererseits bietet die verschlüsselte Struktur für Journalisten, Verfolgte oder politisch Oppositionelle die Möglichkeit, auf regional gesperrte Inhalte zuzugreifen, Zensur zu umgehen oder mit anderen Menschen zu kommunizieren.

Die Anonymität erlaubt journalistischen Quellen, in einigen Fällen unerkannt zu bleiben und Whistleblowern, ihre Entdeckungen mit der Öffentlichkeit zu teilen. Wie in vielen anderen Fällen stehen Deep Web und Darknet für etwas, das sowohl für nützliche als auch für schädliche Zwecke genutzt werden kann.

Darknet – was ist erlaubt, wann mache ich mich strafbar?

Das Bewegen im Darknet alleine ist nicht illegal, es stellt jedoch ein Sicherheitsrisiko dar. Durch die vielen Geschichten, die rund um das Darknet kursieren und die Anonymität der Nutzerinnen und Nutzer kommt leicht der Eindruck auf, das Netzwerk sei per se unzulässig. Straffällig werden Sie allerdings nur, wenn Sie illegale Inhalte konsumieren, herunterladen oder rechtswidrige Waren und Dienstleistungen erwerben oder anbieten.

Auch der Verkauf solcher Güter ist unter Strafe gestellt. Hier unterscheidet sich das Darknet kaum von der physischen Welt: Was außerhalb des Internets illegal ist, bleibt es auch im Internet – egal ob im Clear Web oder im Darknet.

Quelle: *Bundesamt für Sicherheit in der Informationstechnik*