Die Dark-Web-Bibel für Anfänger

Einsteigerhandbuch zum Deep Web

HACKER FINDEN.DE Powered by Audat

Disclaimer

Haftungsausschluss
Die dargestellten Inhalte werden mit größtmöglicher Sorgfalt zusammengestellt. Dennoch müssen wir die Haftung für die Vollständigkeit, Richtigkeit und Aktualität der eigenen Informationen, die auf der Website zur Nutzung bereitgehalten werden, ausschließen, es sei denn, wir handeln vorsätzlich oder grobfahrlässig. Der Haftungsausschluss gilt auch für Linksammlungen, die zurzeit Bestehen oder in Zukunft bestehen werden.

Rechtlicher Hinweis
Alle Informationen auf den Seiten dieser Website dienen der allgemeinen Information. Sie stellen keine Rechtsberatung im Einzelfall dar, können und sollen diese auch nicht ersetzen. Alle Informationen auf den Seiten dieser Website dienen der allgemeinen Information. Sie stellen keine Rechtsberatung im Einzelfall dar, können und sollen diese auch nicht ersetzen.

Die Inhalte unserer Website sind urheberrechtlich geschützt. Soweit Sie die Inhalte für Ihre eigenen beruflichen oder persönlichen Zwecke benötigen, räumen wir Ihnen das Recht ein, die bereitgestellten Texte ganz oder teilweise zu speichern und zu drucken.

Die Speicherung und Vervielfältigung von Bildmaterial oder Grafiken aus unserer Website ist nicht gestattet.

Wenn Sie weitere Fragen oder Anmerkungen haben, kontaktieren Sie uns per Mail: hilfe@hacker-finden.de

Was ist Darkweb und wie funktioniert es?

Viele Menschen assoziieren das Dark Web mit dem digitalen Schwarzmarkt, weil alles nur auf illegalem Weg zu beschaffen ist: Drogen, Waffen, Viren und Schadsoftware, Auftragskiller, Gift, Kreditkartennummern, alles Erdenkliche an sensiblen Daten.

Wir positionieren das Darkweb als dunkle Seite des Internets – schließlich steht es auch für anonymes Surfen und damit für illegale Aktivitäten.

Das Dark Web ist ein isoliertes Netzwerk, wohl ein versteckter Bereich des Internets, auf den wir mit einem Standardbrowser nicht zugreifen können. Da Akteure im Dark Web in einem Peer-to-Peer-Overlay-Netzwerk über manuell verschlüsselte Verbindungen miteinander kommunizieren, nutzen sie sogenannte Hidden Services. (versteckte Dienste)

Diese Computer – oder Peers – stellen ihre Funktionalität im Tor-Netzwerk zur Verfügung, das speziell für das Dark Web entwickelt wurde. Die einzelnen Peers dieses Netzwerks können als einfache Webserver oder als komplexe Dienste mit vielen Modulen genutzt werden.

In jedem Fall bauen sie konsequent auf dem WWW als Overlay-Netzwerk auf und werden von dessen Infrastruktur unterstützt. Der gesamte Datenverkehr im Dark Web ist verschlüsselt und daher für Suchmaschinen oder Behörden unsichtbar, einschließlich IP-Adressen, die ansonsten unsere Aktivitäten verfolgen könnten.

Das Darknet als Handelsplattform für Cyber-Kriminalität

Insbesondere die Cyberkriminalität stellt eine ernsthafte Gefahr dar, und die Handelsplattform der Wahl ist natürlich das Darknet, obwohl die „Ware“ und die Motive der Hacker ganz andere sind:

- Hacker, die in erster Linie an persönlichem Gewinn interessiert sind, können alles Interessante anbieten, von Kreditkartendaten bis hin zu den Spezifikationen von Ransomware, die dauerhaften Schaden anrichtet.

- Hinter dem Verkauf von Mitarbeiter-Passwörtern oder anderen Betriebsgeheimnissen kann etwa die Motivation stehen, großen Unternehmen nachhaltig zu schaden.

- Sogenannte „Hacktivisten“ hingegen verfolgen meist politische oder gesellschaftliche Anliegen und hoffen, mit verschiedenen Methoden auf unethische Produktionsbedingungen aufmerksam zu machen.

- Und man sollte nicht unterschätzten: Wir sind in das Zeitalter der Cyberkriegsführung eingetreten.

Die Überwachung von Informationen über die Cyber-Infrastruktur eines anderen Landes gilt als so lukrativ, dass die Bereitstellung ein besonderes politisches Motiv sein kann.

Was passiert mit meinen Daten im Darknet?

Im Internet können Sie sich an die zuständigen und weitere Aufsichtsbehörden wenden. Sowas existiert nicht im Darknet. Es gibt normalerweise keine Betreiber mit Servern in Europa. Dadurch sei es für die Strafverfolgung schwierig, die Daten zu löschen.

Was muss ich tun, wenn ich betroffen bin oder die Wahrscheinlichkeit sehr hoch ist?

- Ändern Sie das Passwort für das betroffene Kundenportal.

- Ändern Sie Ihre Kennwörter auch bei anderen Online-Diensten, wenn Sie dort den gleichen Benutzernamen und das gleiche Passwort verwenden. Generell sollte man immer für jedes Online-Konto ein individuelles und sicheres Kennwort verwenden.

- Überprüfen Sie regelmäßig Ihre Kontoauszüge. Wenn Sie ungewöhnliche Kontobewegungen feststellen, wenden Sie sich bitte umgehend an Ihre Bank. Lassen Sie nicht zu viel Geld auf dem Konto, das Sie für Online-Überweisungen verwenden. Bewahren Sie Ihre Ersparnisse am besten auf einem Sparkonto auf. Sie können auch ein Belastungslimit für Ihr Konto festlegen.

- Löschen Sie verdächtige E-Mails und klicken Sie auf keinen Fall auf Links oder öffnen Sie mitgeschickte Dateianhänge. Kriminelle können damit versuchen, Ihren Computer mit Malware zu infizieren.

- Überlegen Sie, ob Sie sich eventuell eine neue E-Mail-Adresse zulegen wollen.

Womit Sie nach Veröffentlichung Ihrer Daten im Darknet rechnen müssen

- Möglicherweise erhalten Sie seltsame und lästige Anrufe. Sperren Sie unerwünschte Anrufer am besten auf Ihrem Smartphone.

Seien Sie vorsichtig, wenn angeblich ein Mitarbeiter des betreffenden Unternehmens, z.B. Stromanbieter oder der der Polizei, bei Ihnen anruft.

Wichtig: Beenden Sie das Gespräch umgehend. Es handelt sich in diesem Fall mit sehr hoher Wahrscheinlichkeit um einen Betrugsversuch.
Kriminelle wollen auf diese Weise an weitere wichtige Daten wie zum Beispiel Passwörter herankommen.

- Es kann auch zum Identitätsdiebstahl führen. Kriminelle verwenden Ihre E-Mail-Adresse und IBAN-Nummer, um Waren online zu bestellen. Seien Sie also vorsichtig, Ihr Konto kann für Bestellungen belastet werden, die Sie nie aufgegeben haben.

Betrüger können auch in ihrem Namen Verträge abschließen oder Benutzerkonten bei Online-Diensten angelegt werden.

- Betrüger können mit Ihrer IBAN-Nummer Geld im Lastschriftverfahren abbuchen.
- Die gute Nachricht ist: Bei einem Lastschriftverfahren kann das Geld im Verlauf von 13 Monaten zurückgebucht werden.

Seien Sie also wachsam und behalten Sie Ihr Konto im Blick.

SIM-Swapping: So stehlen Hacker ihre Handynummer

Der Grund: Viele Nutzer verknüpfen ihre Handynummer mit Bank-, E-Mail- und Social-Media-Konten. Eine TAN-Nummer für die Online-Überweisung oder ein Sicherheitscode für die Zwei-Faktor-Authentifizierung wird als SMS auf Ihr Smartphone gesendet. Handynummern selbst können nun auch als Passwörter für bestimmte Dienste fungieren. Durch sogenanntes SIM-Swapping versuchen Kriminelle, die Handynummern der Besitzer zu nutzen, um auf deren Konten und Online-Banking zuzugreifen.

So funktioniert SIM-Swapping

Betrüger beschaffen sich über soziale Netzwerke oder gekaufte Datensätze Informationen über Opfer wie Geburtsdatum, Kontonummer oder Wohnort. Zusammen mit der Handynummer des Opfers versuchen Betrüger, online beim Mobilfunkanbieter eine neue SIM-Karte zu bestellen. Im Erfolgsfall erhalten die Betrüger eine neue SIM-Karte mit der alten Handynummer, die den Zugriff auf sensible Daten wie TAN-Nummern für das Online-Banking oder Codes für E-Mail- oder Soziale-Netzwerk-Konten ermöglicht.

Maßnahmen zum Schutz vor SIM-Swapping:

- Hinterlegen Sie bei ihrem Mobilfunkanbieter ein Kundenkennwort für ihre Handynummer. Erst unter Angabe dieses Kennwortes dürfen Service-Mitarbeiter Informationen herausgeben oder eine neue SIM-Karte verschicken.
- Sie können Ihre E-Mail- oder Social-Media-Konten auch mit Zwei-Faktor-Authentifizierung schützen, ohne Ihre Telefonnummer zu speichern. Verwenden Sie dazu ein Authentifizierungsprogramm wie Microsoft Authenticator oder Authy. Das generierte Einmalpasswort wird nur auf dem Gerät angezeigt, auf dem die App installiert ist.

Surfen im Darknet – So funktioniert es

Wer im Dark Web surfen möchte, benötigt Zugang zum Tor-Netzwerk.
Hierfür empfehlen wir die Verwendung des Tor-Browsers, der Firefox verwendet und automatisch alle anderen Tor-Zugriffsfunktionen blockiert. Sie sollten auch für maximale Computersicherheit sorgen.

Unser Tipp: Bitdefender Internet Security

- **Tor Browser für Windows**
- **Tor Browser für macOS**
- **Tor Browser für Linux**
- **Tor Browser für Android App**
- **Onion Browser iPhone- / iPad-App**

Ihre IP-Adresse wird angezeigt, wenn Sie ein Tor-Netzwerk betreten.
Daher empfehlen wir auch VPN-Dienste, die keine Daten protokollieren. Wir empfehlen NordVPN, den aktuellen Testsieger für VPN-Dienste.

Obwohl die ausgefeilte Onion-Routing-Technologie von Tor das Web-Tracking extrem schwierig macht, können Dritte dennoch einige Aspekte Ihrer Web-Aktivitäten ausspionieren. Mit einem VPN können Sie eine Verschlüsselung als weitere Schutzebene einrichten, um Ihre Privatsphäre zu schützen. Gleichzeitig kann ein VPN Ihre IP-Adresse vor Hackern, Ihrem ISP und sogar Regierungsspionen verbergen.

Surfen im Darknet – VPN einrichten

Das Einrichten eines VPNs ist einfach und es gibt mehrere kommerzielle VPNs für Computer und andere Geräte.

So greifen Sie mit einem VPN auf das Dark Web zu:

- **Laden Sie ein sicheres VPN** von einem vertrauenswürdigen Anbieter herunter.

- **Installieren Sie das VPN** auf Ihrem Gerät. Mobile VPNs für sicheres Surfen im Dark Web unter Android oder iOS sind ebenfalls verfügbar.

- **Stellen Sie mithilfe** des VPN-Protokolls in der Liste der Dienstanbietereinstellungen eine Verbindung zu einem VPN-Server her.

- **Starten Sie den Tor-Browser** und durchsuchen Sie ".onion"-Sites mit einer der unten genannten Onion-Suchmaschinen.

Egal ob im Clear Web oder im Dark Web: die Verwendung von Suchmaschinen und anderen Browsing-Tools birgt immer das Risiko von Datenschutzverletzungen, da Ihr Suchverlauf und andere private Informationen preisgegeben werden. Aus diesem Grund ist es wichtig, Online-Sicherheitstools zum Schutz Ihrer persönlichen Daten zu verwenden.

Avast SecureLine VPN verbirgt Ihre IP-Adresse, schützt Ihre WLAN-Verbindung und verschlüsselt Ihre Daten, um Ihre persönlichen Daten online zu schützen.

Die besten Suchmaschinen für das Dark Web

Torch

Torch, ein Kofferwort aus „Tor“ und „search“, bezeichnet die älteste Suchmaschine im Tor-Netzwerk. In Torch sind eine ganze Reihe von Dark-Web-Sites und -Links indexiert. Darüber hinaus gestalten sich Web-Suchen in Torch relativ schnell.
Die Plattform bietet vollständig unzensierte und gefilterte Websuchergebnisse.
Neben einer unbegrenzten Liste von Suchmaschinen bietet Torch auch Web-Tracking-Schutz.

DuckDuckGo

Die Dark-Web-Suchmaschine DuckDuckGo ist sozusagen das Google des Dark Web. Sie gilt als eine der besten privaten Suchmaschinen und ist zur Standardsuchmaschine für Tor Browser geworden.
DuckDuckGo bietet eine einfache Schnittstelle. In der Mitte der Seite befindet sich ein Suchfeld und die Liste der Suchergebnisse ist ähnlich wie bei Google formatiert. **DuckDuckGo** ist nicht auf das Dark Web beschränkt, denn die Suchmaschine deckt auch Clear-Web-Sites ab.
Am wichtigsten ist, dass DuckDuckGo keine Protokolle verwendet, das heißt, dass Ihr Suchverlauf oder andere Benutzerdaten nicht erfasst werden. In Kombination mit einem dedizierten privaten Browser erweist sich DuckDuckGo als leistungsstarke Suchmaschine und effektives Tool zum Schutz der Privatsphäre.

The Hidden Wiki

The Hidden Wiki ist die Dark-Web-Version von Wikipedia. Obwohl es sich nicht wirklich um eine Deep-Web-Suchmaschine handelt, erleichtert sie das Surfen in Tor, indem ein kategorisiertes Verzeichnis mit indexierten Links zu „.onion“-Webseiten und Clear-Web-Links bereitgestellt wird.

Die besten Suchmaschinen für das Dark Web

Ahmia

Bei Ahmia handelt es sich um eine Clear-Web-Suchmaschine, die mit den Onion-Diensten von Tor kompatibel ist. Onion-Sites werden oft mit illegalen Aktivitäten in Verbindung gebracht, aber Ahmia hofft, sie „sozialfreundlich“ zu machen, indem sie Tor-Suchergebnisse filtert und gefälschte oder unsichere Sites entfernt, die möglicherweise Malware enthalten. Die übersichtliche Benutzeroberfläche von Ahmia macht die Suche im Dark Web zugänglicher.

Candle

Candle ist ein Web-Crawler und eine Dark-Web-Suchmaschine für Onion-Webseiten von Tor. Der Candle Index umfasst über 100.000 Seiten, einschließlich Darknet-Handelsseiten und Foren. Aus diesem Grund ist Candle bei Cyberkriminellen und anderen, die illegale Waren im Darknet kaufen, sehr beliebt. Die Suchmaschine von Candle hat sich als effektiv, aber minimalistisch erwiesen und liefert nur die zehn relevantesten Ergebnisse für Ihre Anfrage. Und das Suchfeld kann bestimmte Zeichen wie Klammern oder Anführungszeichen nicht verarbeiten.

Not Evil

Not Evil ist eine Onion-Dark-Web-Suchmaschine, die einen guten Einstiegspunkt für Tor-spezifische Suchtools bietet. Der Name "Not Evil" bezieht sich auf ein altes Google-Motto: "Don't be evil". Aber im Gegensatz zu Google hat es keine Werbung oder Web-Tracking.

Dark Search

Dark Search ist eine relativ neue kostenlose Suchmaschine, die darauf abzielt, das Dark Web zugänglicher zu machen. Diese Dark-Web-Suchmaschine hat eine benutzerfreundliche Oberfläche und bietet kostenlosen Zugriff auf Onion-Links und -Websites.

IT-Hilfe von Experten erhalten

Schnell, einfach & diskret

Wurden Sie gehackt oder erpresst?
Haben Sie den Zugang zu Ihrem Konto verloren?
Müssen Sie sensible Bilder oder Videos entfernen?
Wurde Ihre ID missbraucht?
Wollen Sie eine Beweissicherung für Strafverfolgung?
Möchten Sie Cybermobbing stoppen?
Haben Sie ein Smartphone- oder Computerproblem?
Sind Sie Opfer von Online-Betrug?

Wir helfen Ihr Problem zu lösen

Bei Fragen oder IT-Notfällen einfach ein Online Videogespräch mit einem Experten buchen:
https://www.hacker-finden.de/kontakt/
oder schreiben Sie uns an hilfe@hacker-finden.de

Weitere e-Books: www.hacker-finden.de/ebooks
Weitere Informationen: www.hacker-finden.de

Es gibt Situationen, die sehr fortgeschritten sind und bei denen bestimmte Arten von Online-Schwachstellen oder Hacker-Angriffen die Schadensursache sein können. Wenn die Best-Practice-Schritte nicht zur Behebung führen oder Sie Informationen über den Täter herausfinden wollen, buchen Sie sich eine persönliche kostenlose Ersteinschätzung mit einen Experten:

JETZT STARTEN

HACKER FINDEN.DE Powered by Audat