Parallelwelt mit System:

Struktur, Macht und Gegenwehr im Darknet

Tim Wetterau, axilaris GmbH

Marktplätze, Bewertungen, Dienstleistungsangebote – vieles wirkt vertraut. Unter der Oberfläche operiert jedoch ein System, das sich konsequent der Sichtbarkeit entzieht und dennoch nach klaren ökonomischen Regeln funktioniert. Plattformen verschwinden, neue Netzwerke entstehen, Gruppen professionalisieren sich weiter. Die Dynamik ähnelt der regulären Wirtschaft, nur ohne offizielle Spielregeln. Wie stabil ist diese digitale Parallelstruktur wirklich?

Auf den ersten Blick wirken die Strukturen des Darknets vertraut: Marktplätze, Dienstleister, Bewertungen und Kundenbeziehungen. Bei näherem Hinsehen zeigen sich diese Spiegelbilder jedoch verzerrt und ihrer gewohnten Ordnung entzogen. Transparenz weicht Anonymität, zentrale Kontrolle wird durch verteilte Strukturen ersetzt, und nahezu jede Bewegung scheint sich dem Zugriff von außen zu entziehen. Bekannte Regeln bestehen fort, wirken jedoch unter grundlegend veränderten Bedingungen. Dieser Beitrag unternimmt den Versuch, diese Strukturen greifbarer zu machen. Im Fokus stehen dabei weniger spektakuläre Einzelfälle als vielmehr die zugrunde liegenden Netzwerke, Mechanismen und Dynamiken, die das Darknet zu einem dauerhaften Faktor der digitalen Gegenwart gemacht haben.

Vom Randphänomen zur digitalen Parallelökonomie

Mit dem Begriff Darknet verbinden viele Menschen vor allem das TOR-Netzwerk, ein

Anonymisierungsnetzwerk („The Onion Router“), das Internetverkehr über mehrere verschlüsselte Knotenpunkte leitet, um Herkunft und Identität der Nutzenden zu verschleiern. Tatsächlich existiert jedoch nicht das Darknet, sondern eine Vielzahl unterschiedlicher Netzwerke. Diese Einordnung lässt sich aus der Entstehungsgeschichte erklären: Bereits in den 1970er Jahren versuchte das US-amerikanische Militär, Kommunikationswege außerhalb des öffentlich zugänglichen ARPANETs zu etablieren. Am Grundprinzip hat sich seitdem wenig verändert. Darknets sind nicht öffentlich zugängliche Netzwerke, die nur über spezielle Zugangsverfahren erreichbar sind. [1] Der mediale Begriff „Darknet“ wurde 2003 durch eine wissenschaftliche Arbeit zweier Microsoft-Mitarbeiter geprägt, die mehrere Peer-to-Peer-Netzwerke untersuchten, in denen urheberrechtlich geschütztes Material ausgetauscht wurde. Zu den bekanntesten zählen Napster, Gnutella und eDonkey. [2] Die zunehmende Strafverfolgung machte es notwendig, Mechanismen zur Identitätsverschleierung zu etablieren. In diesem Kontext entstand 2003 auch der erste Code für den heute bekanntesten Darknet-Browser TOR (The Onion Router). [3]

Die Weiterentwicklung des Darknets lässt sich in mehrere Generationen einteilen. Generation 1 wurde maßgeblich durch Silk Road geprägt, den ersten zentralisierten und modernen Darknet-Marktplatz für den Drogenhandel. Bis zur Schließung im Jahr 2013 wurden dort rund 9,5 Millionen Bitcoin mit einem damaligen Gesamtwert von etwa 1,2 Milliarden US-Dollar über pseudonyme Escrow-Systeme gehandelt [4]. Silk Road stellte einen Präzedenzfall dar, der die Machbarkeit anonymer digitaler Märkte belegte und erstmals rechtliche Maßstäbe für die Strafverfolgung setzte.

Nach dem Ende von Silk Road etablierten sich ab 2018 in Generation 2 zahlreiche neue Marktplätze, die ihr Angebot über den reinen Drogenhandel hinaus diversifizierten. Plattformen wie TheRealDeal handelten mit sogenannten Cyberwaffen und Software-Exploits. Dies führte zu vermehrten DDoS-Angriffen (Distributed Denial of Service) zwischen konkurrierenden Märkten, teils auch gegen sich selbst. [5] Staatliche Operationen, insbesondere durch Großbritannien und die USA, sorgten in dieser Phase für zahlreiche Takedowns oder freiwillige Abschaltungen aus Angst vor Deanonymisierung.

Generation 3 ist durch einen deutlichen Trend zur Dezentralisierung geprägt. GPS-Drop-Systeme, bei denen Übergaben physischer Waren über anonymisierte, koordinatenbasierte Ablageorte ohne direkten persönlichen Kontakt organisiert werden, sowie die Verteilung der IT-Infrastruktur sollen die Identität der Nutzenden besser schützen. Sichtbar wurde diese Entwicklung vor allem durch den russischen Marktplatz Hydra, der 2021 einen Jahresumsatz von rund 2,6 Milliarden US-Dollar erzielte und damit seine Marktdominanz unter Beweis stellte. [6] Neben klassischen Handelsgütern etablierten sich zunehmend Malware-as-a-Service-Angebote, also arbeitsteilige Geschäftsmodelle, bei denen Schadsoftware von spezialisierten Entwicklergruppen erstellt und gegen Beteiligung an den Erlösen oder feste Gebühren an andere Kriminelle vermietet wird. Mit dem Takedown im Jahr 2024 markiert Hydra den letzten großen zentralen Marktplatz dieser Generation.

Im Jahr 2025 ist das Darknet kein einheitlicher Raum mehr, sondern besteht aus vielen kleineren, teils regional geprägten Netzwerken mit unterschiedlicher technischer Infrastruktur. Dennoch nutzen täglich rund drei Millionen Menschen das TOR-Netzwerk, was die anhaltende Bedeutung dieser verborgenen Online-Strukturen zeigt.

Da Transaktionen mit Bitcoin inzwischen deutlich besser von Ermittlungsbehörden nachverfolgt werden können, weichen viele Akteure auf stärker anonymisierte Kryptowährungen wie Monero aus. Gleichzeitig werden klassische Treuhand-Systeme, bei denen eine Plattform das Geld bis zum Abschluss eines Geschäfts verwaltet, zunehmend durch technische Verfahren ersetzt, die ohne zentrale Kontrollinstanz auskommen und weniger

Tim Wetterau

Tim Wetterau ist Spezialist für Cybersicherheit bei der axilaris GmbH in Chemnitz, einem IT-Dienstleister für individuelle IT-Lösungen und Cloud-Infrastrukturen. Durch sein fünfjähriges Studium im Bereich Digitale Forensik und Cybercrime ist er mit einer Vielzahl von Angriffsmethoden vertraut. Nach einer Lehrtätigkeit an der Hochschule Mittweida begann er 2024 seine Tätigkeit bei axilaris und betreut mit seinem Team Kund:innen bei der Verbesserung ihrer IT-Sicherheit im Unternehmen.

Kontakt

t.wetterau@axilaris.de

www.axilaris.de

Cyberkriminalität im Darknet hat sich von einem technischen Randphänomen zu einer hochprofessionellen und resilienten Parallelökonomie entwickelt.

Einblick in die Transaktionen erlauben. Dadurch werden die Märkte widerstandsfähiger gegenüber Abschaltungen und Ermittlungen.

Vortrieb durch Professionalisierung

Das Darknet besteht aus einer Vielzahl einzelner Netzwerke. Die dort agierenden Akteure sind jedoch kaum noch Einzelpersonen, sondern stark in Gruppen organisiert. Seit dem Wegfall großer Marktplätze vernetzen sich viele kleinere Märkte untereinander, kooperieren situativ und konkurrieren zugleich. [7] Diese Inter-Netzwerkkoordination ist ein zentraler Treiber für die hohe Persistenz des Systems trotz starker Volatilität. Anstatt sich auf einzelne Plattformen zu verlassen, agieren Märkte als lose verbundene Knoten. Bewertungs- und Reputationssysteme werden plattformübergreifend übertragen, um Anbieter- und Kundschaftmigration zu erleichtern. [8]

Eine zentrale Rolle spielt die Professionalisierung der Cyberkriminalität. Mit LockBit als Vorreiter des Ransomware-as-a-Service-Modells etablierte sich seit 2019 ein arbeitsteiliges cyberkriminelles Geschäftsmodell, bei dem Entwickler ihren Schadcode an andere Gruppen vermieten. [9] Neben der reinen Verschlüsselung von Systemen steht zunehmend die Exfiltration sensibler Daten im Vordergrund, die anschließend gewinnbringend weiterverkauft werden. LockBit agiert dabei mit klar definierten Rollen, darunter Entwickelnde, Distributoren, Affiliates und Geldwäsche-Netzwerke.

Ein weiterer Professionalisierungsschritt zeigt sich in der Bildung krimineller Zusammenschlüsse. Seit September 2025 kooperiert LockBit 5.0 mit den Gruppen Qilin und DragonForce. Diese kartellartige Organisation erlaubt das Teilen technischer Ressourcen und gegenseitige Unterstützung. Während dies die Stabilität der Akteure erhöht, steigt zugleich das Schadenspotenzial für Opfer erheblich. [10]

Ökonomische Kennzahlen lassen sich nur näherungsweise erfassen. Den größten Anteil der Underground Economy bilden weiterhin illegaler Drogenhandel und Cyberkriminalität. Der Drogenhandel bleibt mit rund zwei Milliarden US-Dollar jährlich führend, begünstigt durch die Entstehung zahlreicher kleiner Märkte nach der Schließung von Hydra. Parallel diversifiziert sich die Cyberkriminalität stark, wie in Abbildung 1 zu sehen ist: Der Handel mit gestohlenen Daten und gefälschten Identitäten, Ransomware, Hacking-Tools und Angriffsdienstleistungen dominiert neben dem Drogenhandel, ergänzt durch Services wie Geldwäsche. Schätzungen zufolge wurden 2025 rund 25 Milliarden kompromittierte Zugangsdaten im Darknet gehandelt. [11]

Dezentralisierung, Plattformlogiken und arbeitsteilige Geschäftsmodelle erschweren staatliche Gegenmaßnahmen nachhaltig.

Geopolitik und staatliche Dimensionen

Trotz zunehmender Professionalisierung gelingt es internationalen Strafverfolgungsbehörden weiterhin, Darknet-Plattformen gezielt anzugreifen. Organisationen wie Europol und das FBI setzen dabei auf koordinierte, staatlich getragene Operationen.

Ein historischer Einschnitt war der Schlag gegen Hydra im April 2022. Das Handelsvolumen aller Darknet-Märkte brach daraufhin kurzfristig um rund 90 Prozent ein. Zudem wurden tausende Bitcoin-Wallets beschlagnahmt, zahlreiche Akteure festgenommen und Millionen Nutzendenkonten gesperrt. [12] Auch 2025 kam es zu umfangreichen Maßnahmen, insbesondere durch die Operation RapTor, bei der international über einhundert Festnahmen sowie erhebliche Bargeld-, Drogen- und Waffenfunde verzeichnet wurden.

Diese Erfolge verdeutlichen die Wirksamkeit internationaler Zusammenarbeit. Gleichzeitig zeigen sie, dass selbst massive Takedowns die strukturelle Dynamik der Underground Economy nur temporär beeinflussen. Dezentralisierung und Fragmentierung

bleiben zentrale Herausforderungen für staatliche Akteure. [13]

Bedrohungslandschaft 2026+: Prognose zur Entwicklung des Darknets

Die zukünftige Entwicklung des Darknets ist schwer vorhersehbar, dennoch zeichnen sich klare Trends ab. Kartellartige Zusammenschlüsse wie bei LockBit erhöhen die Widerstandsfähigkeit gegen Strafverfolgung. Dezentralisierte TOR-Infrastrukturen, Invite-only-Marktplätze und Blockchain-basierte Architekturen erschweren gezielte Takedowns zusätzlich.

Besonders Ransomware bleibt eine der größten Bedrohungen für Unternehmen weltweit. Angriffsmuster entwickeln sich von Double- zu Triple-Erpressungen weiter, bei denen neben Verschlüsselung auch Datenveröffentlichung und DDoS-Angriffe angedroht werden. [14] Beobachtungen von axilaris deuten zudem auf eine Zunahme persönlicher Erpressungsversuche hin, etwa durch direkte Kontaktaufnahme mit den Angegriffenen.

Diese Entwicklung hängt auch mit der sinkenden Zahlungsbereitschaft der Opfer zusammen. Während 2023 noch rund 1,1 Milliarden US-Dollar an Lösegeld erpresst wurden, sank dieser Wert 2025 auf etwa 530 Millionen US-Dollar. [15]

Multidisziplinäre Schutzaspekte

Ein wirksamer Schutz vor Darknet-basierter Cyberkriminalität setzt einen ganzheitlichen Ansatz voraus. Die axilaris GmbH aus Chemnitz orientiert sich dabei an einem Modell, das technische, organisatorische und personelle Aspekte miteinander verbindet.

Auf technischer Ebene gehören dazu unter anderem Systeme zur Angriffserkennung und -reaktion (Detection & Response), die Auswertung öffentlich zugänglicher Informationen (OSINT), gezielte Suche nach versteckten Bedrohungen im eigenen Netzwerk (Threat Hunting) sowie regelmäßige Penetrationstests zur Überprüfung der IT-Sicherheit. Organisatorisch stehen die Einhaltung regulatorischer Vorgaben, Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebs im Krisenfall (Business Continuity Management) sowie strukturierte Notfall- und Krisenübungen im Fokus.

Der Faktor Mensch bleibt dabei entscheidend. Mitarbeitende sind häufig das schwächste Glied in der Sicherheitskette. Regelmäßige Awareness-Schulungen und Phishing-Simulationen sind daher essenziell, um Risiken sichtbar zu machen und das Sicherheitsniveau nachhaltig zu erhöhen.

Fazit

Wer heute noch darauf hofft, unter dem Radar zu bleiben, unterschätzt die Professionalität moderner Angreifergruppen. In einer zunehmend vernetzten Bedrohungslandschaft reichen punktuelle Sicherheitsmaßnahmen nicht mehr aus. Entscheidend ist die Fähigkeit, Angriffe frühzeitig zu erkennen, strukturiert zu bewältigen und den Geschäftsbetrieb auch unter Druck aufrechtzuerhalten. ■

Kurz und Bündig

Das Darknet hat sich von frühen Peer-to-Peer-Strukturen zu einer global vernetzten Parallelökonomie entwickelt. Drei Generationen von Marktplätzen zeigen den Wandel von zentralen Plattformen wie Silk Road und Hydra hin zu dezentralen, fragmentierten Netzwerken. Ransomware-as-a-Service und kartellartige Zusammenschlüsse erhöhen die Professionalität krimineller Gruppen. Staatliche Takedowns führen nur temporär zu Einbrüchen. Rund drei Millionen tägliche TOR-Nutzende unterstreichen die anhaltende Relevanz.

Weitere Infos zum Artikel finden Sie unter folgendem Link: https://bit.ly/4cNtH3i