Prof. Dr. Hendrik Siegmund

Hendrik Siegmund absolvierte in den Jahren 1984-1999 ein naturwissenschaftliches Studium, das er mit Promotion abschloss; anschließend war er als wissenschaftlicher Mitarbeiter tätig. Von 2000 bis 2005 war er Autor im IT-Bereich, Dozent und Consultant bei einer IT-Beratungsfirma, von 2005 bis 2007 IT-Systemadministrator in einem mittelständischen Industrieunternehmen. In den Jahren 2007-2019 war Hendrik Siegmund IT-Leiter im Diakonischen Werk Innere Mission Leipzig e. V.. 2016 schloss Siegmund noch ein berufsbegleitendes Studium zum Master Sozialinformatik erfolgreich ab. Seit April 2020 ist Professor Siegmund Dozent für Technische Informatik am Standort Leipzig der Berufsakademie Sachsen.

Kontakt: hendrik.siegmund@ba-sachsen.de

Das Darknet: Alles finster – oder nicht?

Hendrik Siegmund

Die Medienberichterstattung und einige an einzelne Interessengruppen adressierte Veröffentlichungen assoziieren mit dem Begriff Darknet vor allem kriminelle und bedrohliche Aktivitäten. Eine nähere Betrachtung verfügbarer Statistiken und Analysen offenbart jedoch ein differenzierteres Bild, das die emotional empfundene Bedrohlichkeit relativiert: Nur ein kleiner Teil der Nutzer des Darknets greift tatsächlich auf illegale Angebote zu. Allerdings steht außer Frage, dass einige illegale Aktivitäten, die sich anonymisierende Technologien des Darknets zunutze machen, vorsätzlich erhebliche materielle und immaterielle Schäden anrichten. Es bleibt daher für Unternehmen und Organisationen dringend erforderlich, das eigene Netzwerk und die in IT-Systemen verarbeiteten Informationen angemessen zu schützen. Dazu gehören u.a. inhaltliche Kontrollen des Datenverkehrs auf der obligatorischen Firewall am Übergang zum öffentlichen Internet und insbesondere für Betreiber kritischer Infrastrukturen ab 2023 auch Systeme zur Angriffserkennung.

Media coverage and a number of publications addressed to individual interest groups mainly associate the term darknet with criminal and threatening activities. A closer examination of available statistics and analyses, however, reveals a more differentiated picture that relativizes the emotionally perceived threat: Only a small proportion of darknet users actually access illegal services. There is, however, no doubt that some illegal activities that take advantage of anonymizing darknet technologies intentionally cause considerable material and immaterial damage. It therefore remains imperative for companies and organizations to adequately protect their own network and the information processed in IT systems. This includes, for example, controlling the content of data traffic on the mandatory firewall at the interface to the public Internet and, in particular for operators of critical infrastructures, the implementation of attack detection systems as of 2023.

Der Begriff Darknet

Die meisten von uns besitzen vom Darknet zwar eine wenn auch vage Vorstellung, eine präzise Begriffsbestimmung ist jedoch schwierig und unterliegt einem zügigen zeitlichen Wandel. Die mit „dem Darknet“ verbundenen Inhalte und Ressourcen sowie die aus seinem „Schutz“ heraus unternommenen Aktivitäten verändern sich kontinuierlich, und mit ihnen auch die Bedeutung des Begriffs. Ursprünglich gewählt als Sammelbegriff für alle lokalen Netzwerke, die vom ARPANET als Vorläufer des Internets aus nicht erreichbar waren [vgl. Mirea et al. 2019], besaß die Bezeichnung zunächst noch keinerlei negative Konnotation. Die heute verbreitete Assoziation des Darknets mit kriminellen Aktivitäten ergab sich allerdings bereits um die Jahrtausendwende: Aus immer mehr privaten, geschlossenen Peer-to-Peer-Netzwerken heraus formte sich der illegale Austausch von Audio- und Videodateien oder lizenzrechtlich geschützter Software über das Internet als Hauptzweck dieser Darknets heraus [Biddle et al. 2002]. Ab etwa 2010 vollzog sich ein weiterer Bedeutungswandel, initiiert einerseits durch die Verknüpfung mit neuen, eigentlich zu anderen Zwecken entwickelten Anonymisierungstechnologien und andererseits durch die wachsende Kommerzialisierung legaler und illegaler Angebote – einschließlich deren durch Kryptowährungen ermöglichten anonymen Bezahlung [Platzer et al. 2020].

Gegenwärtig verstehen wir unter dem Darknet, wiederum zusammenfassend für viele verteilte Netze, einen Teil der über das Internet erreichbaren Ressourcen und Dienste, die versteckt, nicht öffentlich und nicht schrankenlos zugänglich sind. Der Zugang ist nur unter Einsatz von Anonymisierungstechnologien wie dem Tor-Netzwerk möglich, die sowohl die Anonymität der Nutzer als auch der Anbieter bis zu einem gewissen Grad schützen können. Dabei spielt es keine Rolle, ob die Angebote als kommerziell, nicht kommerziell, legal oder kriminell einzustufen sind. Vielfach ist es lediglich diese Schutzfunktion, die Nutzer zur Verwendung des Tor-Netzwerks motiviert, insbesondere in Ländern mit aktiver Zensur des Internets. Dort fällt die Nutzung illegaler Angebote anteilig sogar messbar geringer aus [Jardine et al. 2020].

Es liegt also nahe, die Definition des Begriffs Darknet weniger an den Inhalten als vielmehr an der verwendeten Technologie zu orientieren. Ein solches technologiebasiertes Verständnis des Darknets, das schon von Mansfield-Devine [2009] angeregt wurde, vertreten aktuell u.a. auch Platzer et al. [2020]. Es soll den Begriff von der Frage der Legalität angebotener Dienste entkoppeln. Dies erscheint im Interesse einer Versachlichung der Diskussion auch durchaus geboten: Mirea et al. [2019] nennen mehrere Beispiele dafür, dass die aktuelle Medienberichterstattung zur einseitigen Betonung krimineller Aktivitäten im Darknet tendiert – eine Beobachtung, die ebenso auch auf Veröffentlichungen für bestimmte Interessengruppen zutrifft wie etwa Vogt [2017] mit Zuschnitt auf die Zielgruppe Kriminalpolizei. Eine Objektivierung der Berichterstattung und eine klare Abgrenzung gegenüber weiteren ähnlichen Begriffen erscheint daher wünschenswert.

Weitere Begriffe und Nutzungszahlen

Im Zusammenhang mit dem Darknet werden regelmäßig Begriffe wie Deep Web und Dark Web verwendet, oft fälschlicherweise sogar als Synonyme [Hatta 2020]. Zwischen Darknet und Dark Web besteht auch, analog zum Verhältnis von World Wide Web zum Internet, tatsächlich eine Überschneidung. Das Darknet kann aus technischer Sicht alle Dienste und Technologien des Internets anbieten, also z.B. E-Mail-Dienste oder Dateiübertragung mit ihren jeweiligen Protokollen. Das World Wide Web ist dagegen auf Ressourcen und Dienste beschränkt, die das Protokoll HTTPS und vereinzelt noch das ältere, nicht durch Transportverschlüsselung geschützte HTTP verwenden [vgl. Platzer et al. 2020]. Das Dark Web wäre folglich technisch definiert nur eine Teilmenge des Darknets.

Etwas anders stellt sich die Situation für den Terminus Deep Web dar. Er wurde von Bergmann [2001] eingeführt, um die für normale Suchmaschinen sichtbaren und öffentlich zugänglichen Internetressourcen von unsichtbaren bzw. nichtöffentlichen Teilen abzugrenzen. Mit dem Begriff Deep Web war und ist in diesem Sinn keine negative Bedeutung verknüpft. Es handelt sich vielmehr überwiegend um private, unternehmens- oder organisationsinterne Informationen und Dienste, die zwar über das Internet erreichbar, aber nicht für die Öffentlichkeit bestimmt sind. Dazu gehören Unternehmens-, Wissenschafts- oder Bibliotheksdatenbanken, Online-Banking oder Soziale Medien. Gemeinsam ist diesen Ressourcen, dass sie für den Zugriff eine Anmeldung mit persönlichen Zugangsdaten erfordern. Ohne solche Zugangsdaten können auch Suchmaschinen Inhalte des Deep Webs nicht indexieren, und dies ist einer der Gründe für die Unsichtbarkeit dieser Dienste im öffentlich zugänglichen Surface Web. Grundsätzliche technische Unterschiede bestehen zwischen Deep Web und Surface Web nicht, Ressourcen in beiden Bereichen des Internets lassen sich mit den gleichen Browsern und Protokollen erreichen.

Das Darknet wird oft als Teil des Deep Web bezeichnet, weil es ebenfalls nicht von Suchmaschinen indexiert werden kann. Gemäß der weiter oben vorgenommenen technologiebetonten Definition ist dies jedoch nicht ganz zutreffend, weil zum Darknet die Nutzung einer zusätzlichen Anonymisierungstechnologie gehört, und mit dem Begriff Web wieder eine technologische Einschränkung auf bestimmte Dienste vorgenommen würde.

Im Interesse einer sachlichen Diskussion kann es außerdem instruktiv sein, sich mit den Größenverhältnissen der einzelnen Bereiche des Internets und den jeweiligen Nutzerzahlen zu beschäftigen. 2001 umfasste das Deep Web 400-550mal so viele Informationen wie das öffentliche Surface Web [Bergman 2001]. Aktuelle Schätzungen gehen davon aus, dass etwa 90% der Internetressourcen zum Deep Web gehören [BSI 2022] und damit für Suchmaschinen unerreichbar sind. Daraus folgt, dass sich Surface Web und Darknet die verbleibenden etwa 10% der Ressourcen teilen. Verlässliche Angaben sind allerdings kaum verfügbar, die veröffentlichten Zahlen zum Anteil des Surface Webs liegen zwischen 0,03% [Grannan 2013] und 4-16% [Rudesill et al. 2015]. Ähnlich weit liegen die Angaben zum Darknet auseinander, sie reichen von 0,01% für das Dark Web [Grannan 2013] bis 5% [Rudesill et al. 2015]. Ursachen für diese Variationsbreite lassen sich sowohl in der nicht ohne Weiteres greifbaren Natur des Forschungsgegenstandes selbst als auch in verschiedenen Metriken vermuten, die zur Berechnung des Anteils herangezogen werden. Soweit überhaupt angegeben, kommen hierfür das gespeicherte Datenvolumen [Bergman 2001], die Anzahl der Websites oder auch die Anzahl der Nutzer des Tor-Browsers zur Anwendung [Jardine et al. 2020]. Abb. 1 veranschaulicht die angenäherten Anteile von Surface Web, Deep Web und Darknet, hier anstelle der sonst häufig genutzten Eisberg-Analogie mit Hilfe der relevanten Bestandteile eines Apfels. Der Anteil des Darknets ist konservativ mit < 1% angegeben, weil exakte Daten fehlen. Zwar spezifiziert das Tor-Projekt als Betreiber des wichtigsten Anonymisierungsnetzwerks für den Darknet-Zugriff die Anzahl der Darknet-Adressen für Oktober 2022 mit rund 650.000 [Tor Metrics 2022a], aber diese Zahl ist laut dortigen Hinweisen nicht vollständig. Verglichen mit den 1,9 Mrd. aktiven Websites im Dezember 2021 [Ahlgren 2022] ergibt sich jedenfalls mit 0,00034% ein rechnerischer Anteil noch weit unter den von Grannan [2013] genannten 0,01%.

Jardine et al. [2020] konnten ferner zeigen, dass weltweit durchschnittlich nur 6,7% der Nutzer des Tor-Netzwerks tatsächlich die Angebote des Darknets ansteuern. Die überwiegende Mehrheit dieser geschätzt rund 2,6 Millionen Nutzer des Tor-Netzwerks [Statista 2022a] macht sich lediglich dessen Anonymisierungsfunktion zunut-

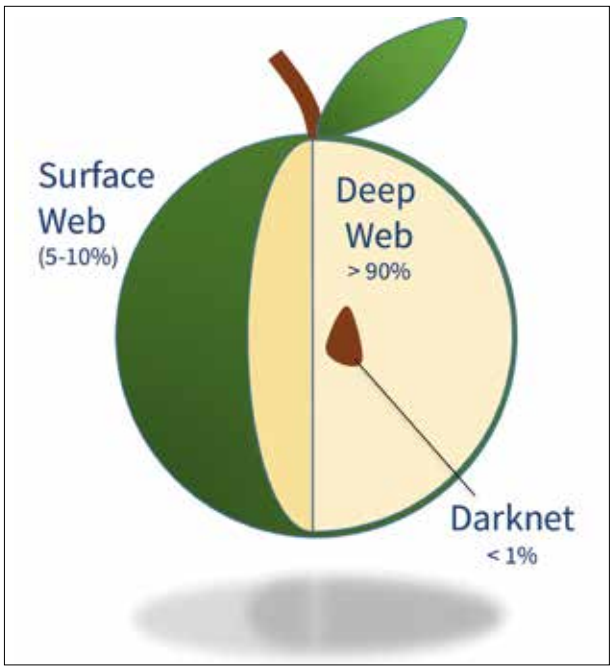

Abb. 1. Teilbereiche des Internets und deren zahlenmäßige Anteile

ze, um im Surface Web zu surfen. Näherungsweise lässt sich daraus auch schließen, wie viele der weltweit 5,25 Mrd. Internetnutzer [Statista 2022b] auf das Darknet zugreifen: Es sind knapp 0,0005%.

Die eingangs diskutierte Überbetonung krimineller Aktivitäten im Darknet und das Heraufbeschwören einer unspezifischen Bedrohung erscheint auf Basis dieser Zahlen nicht gerechtfertigt und sollte im Interesse einer sachlichen, neutralen Berichterstattung vermieden werden. Dies bedeutet jedoch keinesfalls, dass aus der Anonymität des Darknets heraus nicht schwere Angriffe und Straftaten unternommen werden, gegen die Schutzmaßnahmen dringend geboten sind. Bevor diese Maßnahmen erläutert werden, gilt es jedoch, die Technologien zu beleuchten, mit denen die Anonymisierung erreicht wird.

Hidden Services und Anonymisierungstechnologien

Bereits bei der Definition des Darknets wurde festgestellt, dass dessen Ressourcen und Dienste nicht ohne weiteres auffindbar sind und der Zugriff nur unter Nutzung spezieller Anonymisierungstechnologien möglich ist. Dabei sind drei Aspekte von besonderer Bedeutung: Die Lokalisierung von Ressourcen und Diensten im Internet mittels Domain Name Service (DNS), die Erreichbarkeit für Suchmaschinen wie Google oder Bing und die Identifikation von Nutzern und Anbietern über die IP-Adressen ihrer Computer bzw. Internetzugänge. Hinzu kommt dann noch das Verbergen der Inhalte der Kommunikation von Nutzer und Anbieter über eine wirksame Verschlüsselung auf dem Weg durch das Netzwerk.

Um Websites im Internet zu verstecken, bedarf es nicht einmal einer aufwändigen Technologie. Prinzipiell reicht es bereits, auf einen Eintrag der Website im Domain Name Service zu verzichten. Der Zugriff ist damit auf „Wissende“ beschränkt – analog dem Verzicht auf einen Eintrag der eigenen Telefonnummer im Telefonverzeichnis. Nur wer die IP-Adresse oder die Adresse einer Ressource kennt, kann sie kontaktieren. Fehlt der Unified Ressource Locator (URL), also die Webadresse in der verteilten DNS-Datenbank, kann ein normaler Webbrowser nicht mittels DNS-Abfrage die für den Verbindungsaufbau zwingend benötigte IP-Adresse der Website ermitteln. Websites und andere Dienste im Darknet besitzen entweder gar keinen Verzeichniseintrag oder sie bedienen sich in einer separaten Verzeichnisstruktur der Domain „.onion“, die der DNS nicht kennt.

Auch Suchmaschinen sind auf den DNS angewiesen. Sie erstellen einen durchsuchbaren Index aller erreichbaren Websites, den Nutzer zum Auffinden gewünschter Inhalte verwenden [vgl. Stone 2022]. Damit die Suchmaschinen den Inhalt von Websites durchsuchen und in den Index aufnehmen können, müssen sie ebenso wie jeder

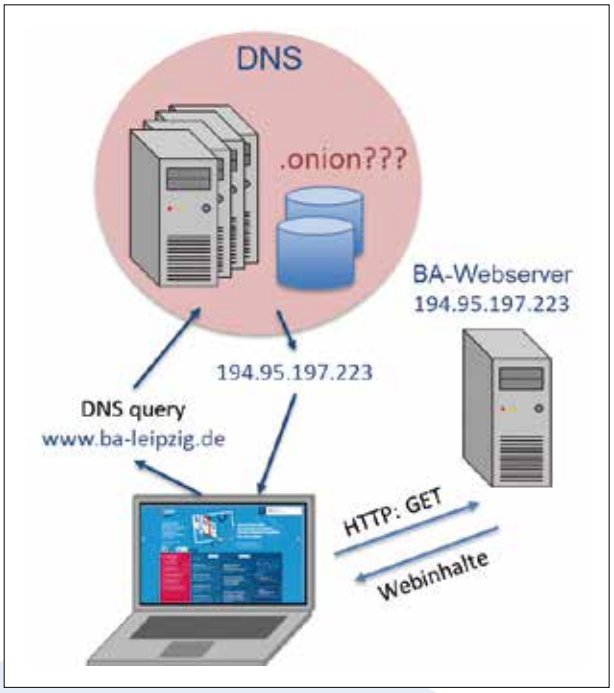

Abb. 2. DNS-Abfrage im Surface Web und Antwort bei bekannter IP-Adresse. Die Domain .onion ist im DNS nicht bekannt.

Webbrowser den URL einer Website in eine IP-Adresse auflösen können. Damit sind nicht im DNS verzeichnete Websites des Darknets für Suchmaschinen ebenfalls nicht erreichbar. Hinzu kommen noch ein Passwortschutz und Verschlüsselung, die im Darknet nicht erwünschte Suchmaschinen endgültig aussperren.

Das bloße Verstecken der Darknet-Ressourcen bietet allerdings noch keine Anonymisierung. Sowohl Anbieter als auch Nutzer benötigen eine eindeutige IP-Adresse für den Datenaustausch über das Internet. Private Anbieter und Nutzer erhalten diese IP-Adresse von Ihrem Internet-Provider, der für jeden seiner Kunden die jeweils zugeordnete IP-Adresse und weitere Informationen zumindest vorübergehend protokolliert. Da der Datenaustausch über das Internet stets die IP-Adressen von Nutzer und Anbieter umfasst, ist niemand im Internet wirklich anonym. Unterstützt wird die Identifikation einzelner Nut-

zer noch durch Daten in Cookies. Dies sind kleine Dateien, die viele Webserver zur persönlichen Konfiguration, Wiedererkennung oder Nachverfolgung der Surf-Aktivitäten auf den Rechnern der Besucher platzieren. Es ist diese Nachverfolgbarkeit und Identifizierbarkeit, die viele Nutzer zum Einsatz einer Anonymisierungstechnologie motiviert [Mirea et al. 2019].

Obwohl es mehrere technische Lösungen gibt, hat sich für die Nutzung des Darknets das Tor-Netzwerk als Anonymisierungswerkzeug etabliert [vgl. Platzer et al. 2020]. Tor steht für The onion router, also frei übersetzt Pfadfinder durch die Zwiebelschalen. Diese wiederum beschreiben ein Netzwerk, das Verbindungen analog einer mehrschaligen Zwiebel nur über mehrere, bei Verbindungsaufbau zufällig gewählte Vermittler (Router oder Nodes) aufbaut. Die Verbindung vom Nutzer bis zum Anbieter umfasst mindestens drei Tor-Nodes. Jeder Streckenabschnitt wird separat verschlüsselt, sodass Nutzer, Anbieter und Nodes jeweils nur ihren nächsten Nachbarn kennen und direkt erreichen. Am Internetzugang des Nutzers ist nicht mehr erkennbar, dass Kontakt mit einem Anbieter im Darknet bestand. Auf Nutzer und Anbieterseite sind als IP-Adressen nur die Adressen des Eingangs- bzw. Ausgangs-Nodes der etwa 6000 Tor-Nodes erkennbar [Tor Metrics 2022b], nicht des tatsächlichen Nutzers oder Anbieters. Mit Ausnahme des letzten Abschnitts zwischen Tor-Netzwerk und Anbieter werden alle transportierten Daten obligatorisch verschlüsselt, sodass zumindest theoretisch im Tor-Netzwerk und bis zum Nutzer weder eine Identifikation der Kommunikationspartner noch ein Mitlesen des Datenstroms möglich sind (Abb. 3). Es liegt auf der Hand, dass diese Art des Verbindungsaufbaus auf Seiten der Nutzer eine besondere Software erfordert. Für den Zugriff auf Darknet-Ressourcen über das Tor-Netzwerk ist der Tor-Browser geeignet, den sich Interessierte frei herunterladen und installieren können.

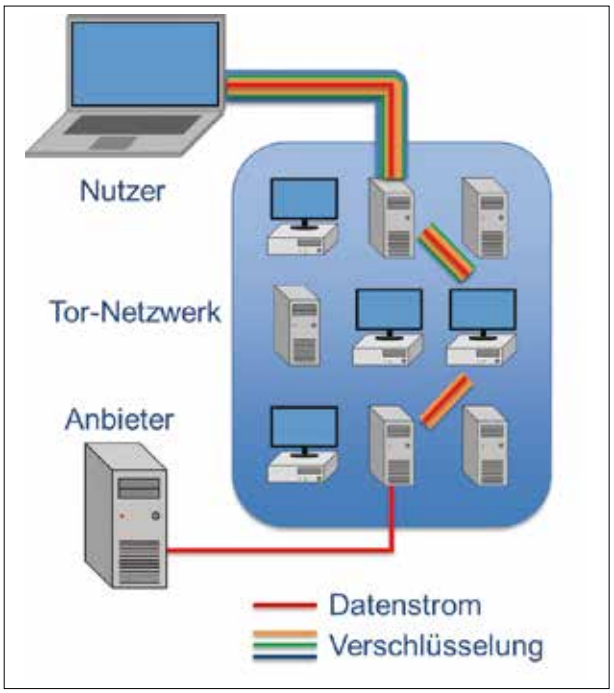

Abb. 3. Anonymisierung und Schutz übertragener Daten durch abschnittsweise Verschlüsselung im Tor-Netzwerk.

Bedrohung und Maßnahmen

Abgesehen von kommerziellen kriminellen Aktivitäten, die mit Waren in der realen Welt verknüpft sind und hier nicht thematisiert werden sollen, bietet sich die Anonymität im Darknet vor allem für die Ausführung von Cyberangriffen an. Das Bundesinnenministerium definiert in seiner aktuellen IT-Sicherheitsstrategie einen Cyberangriff als „…Einwirkung auf ein oder mehrere andere informationstechnische Systeme im oder durch den Cyberraum, die zum Ziel hat, deren IT-Sicherheit durch informationstechnische Mittel ganz oder teilweise zu beeinträchtigen" [BMI 2021]. Diese Angriffe bleiben also auf den virtuellen Raum und digitale Werte beschränkt. Sie nutzen verschiedenste Vektoren, die von Schwachstellen in Soft- und Hardware über Konfigurationsfehler bis zu menschlichen Fehlhandlungen z.B. aufgrund unzureichender Kenntnis reichen [vgl. BMI 2021]. Motive hinter den Angriffen sind häufig die Erpressung von Lösegeld für die Freigabe lahmgelegter IT-Systeme, von Schweigegeld für das Nicht-Veröffentlichten ausgespähter schutzwürdiger Informationen oder auch Spionage als solche [BSI 2021]. Ebenfalls eine wichtige Rolle spielen das gezielte Überlasten von Internetressourcen (Denial of Service Attacke) und Angriffe auf Lieferketten (Supply Chain Attacke). Letztere können dazu führen, dass eine bereits unbemerkt im Herstellungsprozess böswillig manipulierte Software über die normalen Verteilungskanäle für Sicherheitsupdates installiert wird und so eine Vielzahl von Systemen weltweit unbemerkt infizieren kann [vgl. BMI 2021].

Cyberangriffe verursachten bis August 2022 allein in Deutschland einen Schaden von 203 Mrd €, und 84 % der repräsentativ befragten Unternehmen waren bereits von einem Angriff betroffen [Bitkom 2022]. Dagegen ergeben sich zwei wesentliche Ansatzpunkte, die einerseits auf die Ermittlung der Urheber und andererseits auf den Schutz der IT-Systeme möglicher Opfer ausgerichtet sind. Für die Ermittlungsseite sollte dazu den Vorschlägen von Schulze [2019] zufolge vor allem verstärkte Präsenz der Ermittlungsbehörden im Darknet eingesetzt werden. So würde die Übernahme und Stilllegung illegaler Services möglich. Daneben fällt größeren Providern eine besondere Rolle zu. Die durch das Tor Netzwerk gebotene Anonymisierung setzt voraus, dass Datenverkehr über Eingangs- und Ausgangs-Nodes nicht zusammen beobachtet werden kann. In global ausgedehnten Netzen ist diese Annahme wohl zutreffend, aber innerhalb des Netzwerks eines national agierenden Providers nicht mehr. Kann ein einzelner durch sein zeitliches Verlaufsmuster identifizierter Datenstrom auf Eingangs- und Ausgangs-Node beobachtet werden, lassen sich trotz Verschlüsselung der Kommunikationsvorgang nachverfolgen und langfristig auch die Kommunikationspartner identifizieren [Chakravarty et al. 2014]. Jedoch sind diese Ansätze nur erfolgversprechend, wenn tatsächlich Akteure im Darknet ermittelt werden sollen. Bei derzeit offenbar vermehrt aus Russland und China zu beobachtenden Cyberangriffen zur hybriden Kriegsführung [Bitkom 2022] laufen sie ggf. ins Leere.

Umso mehr Bedeutung erlangen Schutzmaßnahmen, die potenzielle Opfer ergreifen können, insbesondere Unternehmen und andere Organisationen. Der aktuelle Lagebericht des BSI zur IT-Sicherheit und das ebenfalls vom BSI herausgegebene Grundschutz-Kompendium liefern vielfältige Hinweise zur Ausrichtung und Ausgestaltung solcher Maßnahmen. Menschliche Fehlhandlungen lassen sich reduzieren, wenn Mitarbeiter einer Organisation für Social Engineering-Angriffe wie Spear Phishing sensibilisiert sind, also dem gezielten persönlich adressierten Versuch, beispielsweise Zugangsdaten zum Netzwerk preiszugeben [BSI 2022b]. Inzwischen selbstverständliche Maßnahmen wie konsequente Datensicherung und die vom Netzwerk getrennte Aufbewahrung der Sicherungsmedien (offline) bieten wirksamen Schutz im Falle einer Ransomware-Attacke, indem sich verschlüsselte Unternehmensdaten aus den Sicherungen wiederherstellen lassen und der Erpressungsversuch schlicht ins Leere läuft [vgl. BSI 2022b]. Der Versuch, die Kommunikation mit Tor-Nodes schon auf der äußeren Firewall über eine Ausschlussliste (Blacklist) der bekannten und vom Tor-Projekt veröffentlichten IP-Adressen der Ausgangs-Nodes wäre dagegen wohl schon aufgrund von deren Vielzahl und Variabilität nicht zielführend. Hier ist gemäß BSI-Grundschutzbaustein „NET.3.2 Firewall“ vielmehr eine inhaltliche Analyse sämtlicher Daten erforderlich, die eine Firewall passieren, zumindest bei eingehendem Netzwerkverkehr einschließlich der eigenen Web-, Mail- oder VPN-Server und auch wenn diese Transportverschlüsselung nutzen [vgl. BSI 2022b]. Schließlich kann bei stärker gefährdeten Organisationen im Rahmen einer Aktualisierung der IT-Sicherheitsstrategie der Einsatz eines verteilten Systems zur Erkennung von Angriffen eingesetzt werden. Solche Intrusion Detection Systems (IDS) werden idealerweise als Kombination aus Netzwerkbasierten Komponenten wie Firewalls und Hostbasierten Komponenten auf geeigneten Servern und Endgeräten eingerichtet. Während die Netzbasierten Komponenten des IDS das gesamte Netzwerkverhalten analysieren, betrachten die Hostbasierten Komponenten das Verhalten der einzelnen Server [vgl. BSI 2002]. Sie können dabei beispielsweise mehrfach gescheiterte Anmeldeversuche mit Zugangsdaten eines Administrators erkennen oder das systematische Öffnen und Schließen von Dateien zur Verschlüsselung durch Schadsoftware. Solche ganzheitlichen Schutzsysteme sind zwar äußerst komplex, aber auch gegen die zunehmenden Advanced Persistent Threats wirksam, die als sorgfältig geplanter, gezielter und hochentwickelter Angriff sonst lange unentdeckt bleiben und daher durch unkontrollierten Datenabfluss großen Schaden anrichten können. Für Organisationen, die dem IT-Sicherheitsgesetz unterliegen, ist der Einsatz eines Systems zur Angriffserkennung gemäß § 8a Absatz 1a BSIG ab 1.5.2023 Pflicht.

Fazit

In vielen Veröffentlichungen wird die kriminelle Seite des Darknets stärker betont als die illegalen Angebote und Nutzerzahlen es rechtfertigen. Dennoch verursachen Cyberangriffe mit möglichen Ursprüngen im Darknet erhebliche Schäden. Gegen die Urheber krimineller Aktivitäten und Angriffe kann mit neuen Ermittlungsmethoden vorgegangen werden. Um potenziell angreifbare Netzwerke zu schützen, müssen darüber hinaus deren Betreiber an die aktuellen Angriffsvektoren angepasste Maßnahmen treffen. Dazu gehört zukünftig auch der Einsatz von Angriffserkennungssystemen, die für Betreiber kritischer Infrastrukturen ab dem kommenden Jahr sogar verpflichtend sind.

Literatur

Ahlgren, Matt (2022): 100 + Internet-Statistiken und Fakten zu 2022. https://www.websiterating.com/de/research/internet-statistics-facts/#chapter-1 Abgerufen am 13.10.2022

Bergman, M. K. (2001): White paper: The deep web: Surfacing hidden value. Journal of Electronic Publishing, 7(1).

Biddle, P.; England, P.; Peinado, M. & Willman, B. (2002): “The darknet and the future of content protection.” In ACM Workshop on digital rights management, S. 155-176., Berlin, Heidelberg (Springer)

Bitkom 2022: 203 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen. https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022 (abgerufen am 17.10.2022)

BMI 2021: Cybersicherheitsstrategie für Deutschland. https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf (abgerufen am 17.10.2022)

BSI 2002: BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen. 1.2 Komponenten und Architektur von IDS. https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/IDS02/gr1_htm.html (abgerufen am 17.10.2022)

BSI 2021: Die Lage der IT-Sicherheit in Deutschland 2021. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf (abgerufen am 17.10.2022)

BSI 2022a: Darknet und Deep Web – wir bringen Licht ins Dunkle. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Darknet-und-Deep-Web/darknet-und-deep-web_node.html (zuletzt abgerufen am 13.10.2022)

BSI 2022b: Grundschutz-Kompendium. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2022.pdf (abgerufen am 17.10.2022)

Chakravarty, S.; Barbera, M.V.; Portokalidis, G.; Polychronakis, M. & Keromytis, A.D. (2014): On the effectiveness of traffic analysis against anonymity networks using flow records. In: International conference on passive and active network measurement, S247-257 Springer, Cham.

Grannan, C. (2020): "What's the Difference Between the Deep Web and the Dark Web?". https://www.britannica.com/story/whats-the-difference-between-the-deep-web-and-the-dark-web. (abgerufen am 13.10.2022)

Hatta, M. (2020): Deep Web, Dark Web, Dark Net: A Taxonomy of "Hidden" Internet. Annals of Business Administrative Science 19 (2020), S. 277-292.

Mansfield-Devine, S. (2009): „Darknets." Computer Fraud & Security, Volume 2009, Issue 12, S. 4-6.

Jardine, E., Lindner, A.M. & Owenson, G. (2020): The potential harms of the Tor anonymity network cluster disproportionately in free countries. https://www.pnas.org/doi/full/10.1073/pnas.2011893117 (abgerufen am 28.8.2022)

Mirea, M.; Wang, V. & Jung, J. (2019): The not so dark side of the darknet: a qualitative study. Security Journal 32: S. 102-118.

Platzer, F.; Landwirth, R.; Wittmer, S.; Yannikos, Y. (2020): Was ist das Darknet? PANDA: Parallelstrukturen, Aktivitätsformen und Nutzerverhalten im Darknet. https://www.sit.fraunhofer.de/fileadmin/dokumente/sonstiges/Whitepaper_Darknet_V4_ES.pdf (abgerufen am 3.8.2022)

Rudesill, D.S.; Caverlee, J. and Sui, D. (2015): The Deep Web and the Darknet: A Look Inside the Inter- net's Massive Black Box. Ohio State Public Law Working Paper No. 314, zitiert in Mirea et al. 2019.

Schulze, M. (2019): Kriminalitätsbekämpfung im Dark Net. SWP-Aktuell 2019 A28, S. 1-8. https://www.swp-berlin.org/publikation/kriminalitaetsbekaempfung-im-dark-net (abgerufen am 8.7.2022)

Statista 2022a: Schätzung zur Anzahl der Nutzer des Tor-Netzwerks pro Tag weltweit von Januar 2018 bis September 2022. https://de.statista.com/statistik/daten/studie/1024020/umfrage/anzahl-der-taeglichen-nutzer-des-tor-netzwerkes-weltweit/ (abgerufen am 13.10.2022)

Statista 2022b: Number of internet and social media users worldwide as of July 2022. https://www.statista.com/statistics/617136/digital-population-worldwide/ (abgerufen am 14.10.2022)

Stone, M. (2022): How Search Engines Work. In: Understanding and Evaluating Search Experience. Synthesis Lectures on Information Concepts, Retrieval, and Services. S. 3-14. Springer, Cham.

Tor Metrics 2022a: Unique .onion services (version 3 only) https://metrics.torproject.org/hidserv-dir-v3-onions-seen.html (abgerufen am 13.10.2022)

Tor Metrics 2022b: Servers. https://metrics.torproject.org/networksize.html (abgerufen am 17.20.2022)

Vogt, Sabine (2017): Das Darknet – Rauschgift, Waffen, Falschgeld, Ausweise – das digitale „Kaufhaus" der Kriminellen? Die Kriminalpolizei 2/2017, S. 4-7.