Presseinformation
Wien, 17. Juni 2019

Darknet: Nur ein Hort des Bösen?

Internationales Forum für Wirtschaftskommunikation erörterte Gefahren und Chancen für Unternehmen und Medien

Für viele ein Mysterium oder der „Hort des Bösen“: das Darknet. Aber: Neben kriminellen Aktivitäten, die auf diesen Seiten stattfinden, bergen die „dunklen Seiten“ des Internets auch Chancen für Unternehmen und für investigative Medien. Das Internationale Forum für Wirtschaftskommunikation (www.ifwk.net) lud Experten aus Wissenschaft, Wirtschaft, Militär und Medien zum Diskurs in den Wiener Speakeasy Club.

Was passiert tatsächlich im sogenannten Darknet? Wie bekommt man Zugang zu diesem Bereich des Internets? Und birgt das Darknet nur Gefahren oder können Unternehmen es legal für ihre Zwecke nutzen? Antworten auf diese spannenden Fragen gab es dieser Tage bei der IFWK-Veranstaltung „Business Risks from the Deep- and Darknet – wenn sich Ihr digitaler Footprint gegen Sie wendet“, zu der IFWK-Präsident **Rudolf J. Melzer** gemeinsam mit **Wilhelm Milchrahm**, Partner und Anwalt bei mslegal, einlud.

Verräterische Spuren im Netz

Wir alle hinterlassen täglich Spuren im Netz. Unser digitaler Fußabdruck ist für potenzielle Angreifer Quelle für kriminelle Aktivitäten, die häufig aus dem Darknet heraus gesteuert werden. 6 % des gesamten Internet-Inhaltes finden sich in diesem sogenannten Darknet, das wiederum Teil des Deep Web ist. Dieses Deep Web besteht großteils aus themenspezifischen Datenbanken und Webseiten, welche von Suchmaschinen nicht indexiert und daher bei einer Suchanfrage nicht gefunden werden. Nur 4 % der Internetinhalte sind im „Surface Web“ zu finden, also jenem Teil des Netzes, der für uns alle frei zugänglich ist.

Wer ins Darknet gelangen will, kann dies tun, braucht aber spezifisches Wissen, erklärt Cybersecurity-Experte und Geschäftsführer von TriConPlus, **Stefan Mausser**. Das bekannteste Darknet ist das TOR (The Onion Router) Netzwerk. Die ersten Konzepte wurden 1995 von der DARPA sowie dem US NAVAL Research Center entwickelt. Im Jahr 2006 wurde „The Torproject“ zu einer Non-Profit Organisation und wird seitdem von einer Community aus Entwicklern, Enthusiasten und Freiwilligen betrieben und weiterentwickelt.

TOR zur Freiheit und Anonymität

Wichtigster Zweck des TOR Netzwerkes war und ist keinesfalls, kriminelle Aktivitäten zu fördern, sondern Anonymität für den Benutzer sicher zu stellen, so Experte Mausser.

Zu den Nutzern zählen sowohl ganz normale User, welche Wert auf ihre Privatsphäre legen als auch „Menschen, die in Ländern mit starker Zensur leben und z.B. blockierte Social-Media-Seiten erreichen

wollen“, so Mausser. Doch auch Aktivisten und Whistleblower greifen gerne auf das Tor Netzwerk zurück, um ihre Identität zu schützen.

IT-Strategie-Expertin **Isabella Mader** vom Excellence Institute bestätigt ebenfalls, dass es zahlreiche Darknet-User mit lauteren Absichten gibt: „Mit dem Zulassen einer immer invasiveren Überwachungsökonomie verdrängen wir Menschen zunehmend in das anonyme Web. In Diktaturen sind es die Menschenrechtsaktivisten, in Europa vielfach jene, die mit ihren legalen Interessen nicht geleakt oder getrackt werden wollen.“

Legales Surfen auf dunklen Seiten

Das Darknet stellt unter anderem sichere Sharing-Plattformen und anonymisierte, abhörsichere Messenger-Dienste bereit. Die meisten TOR-Nutzer kommen aus den USA, Russland und Deutschland. Insgesamt nutzen täglich etwa zwei Millionen Menschen TOR und finden dort auch ganz normale Informations- und Marktangebote.

Grundsätzlich benötigt man den „TOR-Browser“ um auf die Hidden Services im TOR-Netzwerk zuzugreifen. Diese haben speziellen Adressen mit der Endung *.onion und können mit einem gewöhnlichen Webbrowser nicht aufgerufen werden. Laut TOR Statistiken existieren derzeit zwischen 90.000 und 100.000 solcher Adressen.

Milchrahm warnt vor „Gefahrengeneigtheit“

„Das schlichte Surfen im Darknet ist in der Regel legal“, stellt Anwalt Milchrahm klar. „Grundsätzlich gilt ohnedies das allgemeine Strafrecht. Es besteht kein Unterschied, ob Suchtmittel auf der Straße oder online gehandelt werden.“ Im Darknet gebe es allerdings eine gewisse „strafrechtliche Gefahrengeneigtheit“ – etwa dann, wenn man mit Kinderpornografie in Berührung kommt und in Fällen, in denen der schlichte „Besitz“ eine mögliche Straftat nach sich ziehen könne. Ein typisches Beispiel sei der Download einer Hacker-Software: Geschieht dies aus Neugierde oder tatsächlich mit Handlungsvorsatz?

Lässt sich aus dem Besuch des Darknets auf Letzteres schließen? Somit begibt man sich in rechtliche Gefahr. Andererseits, so der Rechtsexperte, gebe das Datenschutzrecht und allgemeine Sorgfaltspflichten vor, dass man sich vor Eindringlingen schützen müsse – das erfordere möglicherweise Kontroll- und Rechercheaktivitäten auch im Darknet. Und gerade Großunternehmen sollten unter Umständen gezielt monitoren, ob etwa ihre Kundendaten im Darknet vorhanden sind. So könne überprüft werden, ob eine unberechtigte Offenlegung von Kundendaten, ein sogenannter data breach, vorliegt, wenn diese im Darknet angeboten werden. „Noch ist hier aber nicht alles rechtlich eindeutig geregelt bzw. ausjudiziert“, weiß Milchrahm. Vieles sei von den Umständen des jeweiligen Einzelfalls abhängig und daher solle in der Regel juristischer Rat eingeholt werden, empfiehlt der Rechtsexperte.

Von Falschgeld bis zum Auftragskiller

Auch Medien- und Aufdeckerplattformen zählen zu den Profiteuren des Darknets. Sie können auf anonym hochgeladenes Whistleblower-Material zugreifen und unter Wahrung der Anonymität umfassend recherchieren.

Wie ein Live-Einstieg Stefan Maussers ins Darknet eindrücklich zeigte, gibt es aber eben auch die „dunkle", kriminelle Seite. Von gefälschten Banknoten, Kreditkarten und Pässen bis zu Drogen und Waffen ist praktisch alles – meist gegen Cryptowährungen – erhältlich. Sogar Auftragskiller können mit wenigen Mausklicks gebucht werden, zeigte der Experte live auf. Und natürlich bieten Hacker ihr illegal gesammeltes Datenmaterial zum Verkauf an.

Ransomware wie Erpressungssoftware, Verschlüsselungstrojaner und andere Schadprogramme sind ebenfalls als Komplett-Packages erhältlich, erfuhren die staunenden Zuhörerinnen und Zuhörer.

Herausforderung für Behörden

Isabella Mader sieht darin auch große Herausforderungen für die öffentliche Hand: „Für Behörden, z.B. für die Exekutive, bedeutet Digitalisierung, dass nicht nur die Wirtschaft in den digitalen Raum migriert, sondern eben auch die Kriminalität. Das Schutzinteresse und der Schutzanspruch z.B. für kritische Infrastruktur gelten dort auch. Mit dieser Challenge ist die Exekutive weltweit konfrontiert. Und sie muss die entsprechenden Rahmenbedingungen schaffen." Europol holt im Kampf gegen die Internetkriminalität allerdings auch stark auf, betonten die Expertinnen und Experten am Podium. In den letzten drei Jahren konnte Europol zahlreiche illegale Märkte im Darknet übernehmen und schließen.

Moderiert wurde die äußerst informative Diskussion von Trending Topics-Redakteurin **Madlen Stottmayr**. Unter den zahlreichen Gästen im Speakeasy Club von **Heidi** und **Lisa Schmerold**: **Rainer Walter**, geschäftsführender Gesellschafter der auf Sicherheits- und Elektrotechnik spezialisierten Pörner GmbH, die bekannten Wirtschaftsjournalisten **Engelbert Washietl** und **Peter Muzik**, **Gabriele Schallegger** von Mondi, **Hatto Käfer** von der Vertretung der Europäischen Kommission in Wien, **Peter Kraus**, Senior Partner bei Hill Woltron, sowie ATOS-Direktor **Herwig Schweng**.

IFWK – seit 2009
2009 gründete Rudolf J. Melzer gemeinsam mit Vertretern der Wirtschaft, Wissenschaft und der Medien das "Internationale Forum für Wirtschaftskommunikation" (IFWK). Das Forum versteht sich als unabhängige Wissens- und Dialogplattform für Opinionleader und Querdenker aus Wirtschaft, Wissenschaft und Medien. Zu den Zielen gehört es unter anderem, neue Denkansätze und Hintergrundinformationen zu wirtschaftsrelevanten Kommunikationsthemen zu vermitteln.

Rückfragehinweis: Melzer PR Group, 1010 Wien
M: office@melzer-pr.com, W: www.melzer-pr.com; www.ifwk.net T: +43-1-526 89 080