Der monatliche Security Awareness Newsletter für Sie

"Dark Web"

Übersicht

Sie haben den Begriff "Dark Web" vielleicht schon einmal gehört, wie er von anderen oder in den Medien verwendet wird, und sich gefragt: "Was ist das Dark Web?" oder "Soll ich diesbezüglich etwas unternehmen?". Heute erklären wir, was das "Dark Web" ist und was es für Sie bedeutet.

Was ist das "Dark Web"?

Das "Dark Web" besteht aus Systemen im Internet, die dazu bestimmt sind, sicher und anonym zu kommunizieren oder derart Informationen zu teilen. Es gibt nicht das EINE "Dark Web"; es ist nicht so etwas wie Facebook, welches von einer einzigen Organisation betrieben wird. Stattdessen besteht das "Dark Web" aus Sammlungen verschiedener Systeme und Netzwerke, die von verschiedenen Personen verwaltet werden und für eine Vielzahl von Zwecken verwendet werden. Diese Systeme sind immer noch mit dem Internet verbunden und Teil des Internets, aber Sie werden sie in der Regel nicht über die normalen Suchmaschinen finden. Oftmals benötigen Sie eine spezielle Software auf Ihrem Computer, um sie zu finden oder darauf zuzugreifen. Ein Beispiel ist das Tor-Projekt. Um auf das Tor "Dark Web" zuzugreifen, laden Sie den Tor-Browser herunter und installieren Sie ihn. Wenn Sie sich über den Tor-Browser mit Webservern verbinden, wird Ihr verschlüsselter Datenverkehr über andere Computer geleitet, die ebenfalls Tor verwenden. Während die Daten sich durch diese Computer bewegen, ändert sich die Quell-IP-Adresse, was bedeutet, dass Ihre Online-Aktivität anonymisiert ist, wenn Sie auf die Website gelangen. Weitere Beispiele für "Dark Webs" sind Zeronet, Freenet und I2P.

Wer verwendet es?

Cyberkriminelle stellen eine große Gruppe von Nutzern des "Dark Web". Sie unterhalten Webseiten und Foren im "Dark Web", um ihre kriminellen Aktivitäten wie den Kauf von Drogen oder den Verkauf von Gigabyte gehackter Daten zu ermöglichen - alles anonym und sicher. Wenn ein Cyberkrimineller beispielsweise eine Bank oder einen Online-Shop hackt, stiehlt er so viele Informationen wie möglich und verkauft diese dann an andere Cyberkriminelle auf Webseiten im "Dark Web".

Es gibt aber auch legitime Gründe zur Nutzung des "Dark Web". Zum Beispiel können Menschen in Ländern, in denen die Zensur grassiert, "Dark Web"-Netzwerke nutzen, um Informationen auszutauschen und zu sehen, was sonst noch in der Welt passiert, während sie ihre Privatsphäre schützen und anonym bleiben. Journalisten, Whistleblower und Personen denen der

Schutz ihrer Daten wichtig ist können das "Dark Web" nutzen, um ihre Anonymität zu erhöhen und Zensur zu umgehen. Darüber hinaus können die genannten Personengruppen diese Technologien, wie den Tor-Browser, nutzen, um nicht nur auf das "Dark Web" zuzugreifen, sondern auch anonym im normalen Internet zu surfen.

Was sollten Sie tun?

Sofern Sie keinen bestimmten Grund haben, auf das "Dark Web" zuzugreifen, raten wir Ihnen davon ab dies zu tun. Einige Webseiten im "Dark Web" werden für illegale Zwecke verwendet, viele der Webseiten verwenden Ihren Computer in einem Peer-Netzwerk, um ihre Ziele zu erreichen, und in einigen Fällen kann Ihr Computer sogar untersucht oder angegriffen werden. Einige Unternehmen bieten Dienste zur Überwachung des "Dark Webs" an, um Sie darüber zu informieren, ob Ihr Name oder andere Informationen von Cyberkriminellen gestohlen und dort gefunden wurden. Der tatsächliche Wert dieser Dienstleistungen ist fraglich. Der beste Weg, sich selbst zu schützen, ist anzunehmen, dass sich einige Ihrer Informationen bereits im "Dark Web" befinden und von Cyberkriminellen genutzt werden. Daraus ergibt sich . . .

- **Seien Sie misstrauisch gegenüber Telefonaten oder E-Mails, die vorgeben, eine offizielle Organisation zu sein und Sie dazu drängen, eine Maßnahme zu ergreifen, wie z.B. eine Geldstrafe zu zahlen. Kriminelle können sogar Informationen, die sie über Sie gefunden haben, verwenden, um einen personalisierten Angriff auszuarbeiten.**
- **Überwachen Sie Ihre Kreditkarten- und Kontoauszüge. Sie können sich auch Benachrichtigungen über alle auftretenden Transaktionen einrichten. Auf diese Weise können Sie erkennen, ob ein Finanzbetrug stattfindet. Wenn Sie etwas bemerken, melden Sie es sofort Ihrem Kreditkartenunternehmen oder ihrer Bank.**
- **Setzen Sie Limits auf Ihre Konten, z.B. nicht mehr als 1.000€ pro Transaktion. Es hat nur minimalen Einfluss darauf, wie Sie Ihre Kreditkarte verwenden können und ist einer der effektivsten Schritte, die Sie unternehmen können, um sich vor Identitätsdiebstahl zu schützen.**

Gastredakteur

Micah Hoffman *(@WebBreacher) ist der leitende Ermittler bei Spotlight Infosec LLC, ein zertifizierter SANS Institute Dozent und der Autor für die SANS OSINT Kurse. Micahs Leidenschaft für Cyber- und Open Source Aufklärung zeigt sich in seinen Projekten, Kursunterlagen und seinem Unterrichtsstil.*

Weiterführende Informationen

Personalisierte Angriffe:	https://www.sans.org/security-awareness-training/resources/personalized-scams
Social Engineering:	https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering
	https://bsi-fuer-buerger.de/BSIFB/DE/Risiken/ID-Diebstahl/Schutzmassnahmen/id-dieb_schutz_node.html
Credit Freeze:	https://sicherbezahlen.de/ueberweisungslimit/
Tor Browser:	https://www.torproject.org/
SANS OSINT Kurs:	https://sans.org/sec487