Szene-Trends nachgefragt – zum Thema: Cybersicherheit versus Cyberkriminalität

Die dunklen Seiten des Internets

Ein Tor, wer sich im Zeitalter von Digitalisierung und Big Data nicht mit DeepWeb und Darknet beschäftigt. Legitimes und notwendiges Anonymisierungsstreben muss sich dabei von den dunklen Seiten des Internets, von schwarzen Märkten und Cyberkriminalität, absetzen. JavaSPEKTRUM-Redakteurin Annegret Handel-Kempf (AHK) fragte bei Udo Schneider, Security Evangelist D-A-CH bei Trend Micro, nach.

Udo Schneider, Security Evangelist D-A-CH, ist seit Jahren auf vielen IT-Veranstaltungen anzutreffen. Der Münchner kennt sich aus mit den Gefahren, die im Internet lauern, und weiß, wie man sich vor ihnen schützen kann. Bevor er beim IT-Sicherheitsanbieter Trend Micro seine jetzige Position als Security Evangelist für den deutschsprachigen Raum (D-A-CH) antrat, beschäftigte er sich als Solution Architect EMEA mehrere Jahre lang mit der Entwicklung geeigneter Maßnahmen gegen diese Gefahren – mit Fokus auf Cloud-Computing, Virtualisierung, Verschlüsselung und Netzwerksicherheit. Schneider kommt dabei seine langjährige Erfahrung zugute, die er als Berater, Trainer und Security-Analyst bei verschiedenen Anbietern des IT-Sicherheitsmarktes erworben hat.

AHK: Herr Schneider, wie kommt es, dass der deutschsprachige, cyberkriminelle Untergrund der am weitesten entwickelte in der EU ist?

Udo Schneider: Obwohl es auch durchaus Untergrundmärkte in anderen EU-Ländern gibt, ist der deutsche Untergrundmarkt der größte, rein in der EU agierende Untergrundmarkt. Zum Beispiel französisch- oder spanischsprachige Märkte sind oft länderübergreifend auch außerhalb der EU, zum Beispiel nach Lateinamerika, ausgerichtet.

Welche Charakteristika, Foren und Marktplätze kennzeichnen den cyberkriminellen Untergrund hierzulande?

Obwohl alle „wichtigen" Waren, zum Beispiel geklaute Kreditkarten, Konten oder Schadsoftware, auch im deutschen Untergrund erhältlich sind, ist die „Auswahl" geringer als in den russischen oder englischsprachigen Märkten.

Dies lässt darauf schließen, dass deutsche Cyberkriminelle für „Massenartikel" auch andere Märkte frequentieren, da es diese dort günstiger gibt. Für Käufer, die der entsprechenden Sprache nicht mächtig sind, tummeln sich im deutschen Untergrund aber auch „Wiederverkäufer", die Leistungen anderer Märkte gegen einen Obolus „in Deutsch" weiterverkaufen.

Dies führt dazu, dass der deutsche Untergrundmarkt sich entsprechende Nischen geschaffen hat, in denen spezielle „regionale" Produkte und Dienstleistungen angeboten werden.

Dies umfasst zum Beispiel Anruf-(Callcenter)-Dienste in deutscher Sprache oder auch die Nutzung spezieller „Dropping"-Taktiken. Im Gegensatz zu anderen Regionen steht beim „Droppen" von Waren mit Hilfe von (gestohlenen) Packstationszugängen in Deutschland eine anonyme, bequeme und weit verbreitete Alternative zu Verfügung.

„Für Java gibt es Libraries, die es Applikationen erlauben, direkt TOR zu nutzen"

In welchem Zusammenhang stehen der „U-Markt" beziehungsweise „Schwarzmarkt", das DeepWeb und das Darknet? Wie sind sie jeweils definiert?

Als „DeepWeb" bezeichnet man allgemein Inhalte, die zum Beispiel nicht über Suchmaschinen des normalen „Surface"-Web auffindbar sind. Dies können im einfachsten Fall zum Beispiel passwortgeschützte Seiten sein, die nur einem geschlossenen Benutzerkreis zugänglich sind. (Universitäts-)Bibliotheken sind dafür ein gutes Beispiel: Obwohl sie massive Informationen (Bücher, Paper, Referenzen) enthalten, sind diese für Normalverbraucher und Suchmaschinen schlichtweg nicht sicht- beziehungsweise durchsuchbar. Inhalte im DeepWeb werden also nicht „mit Absicht" versteckt, sondern sind häufig einfach nur für einen bestimmten Personenkreis zugänglich.

Das „Darknet" wiederum ist für Nicht-Eingeweihte schlichtweg unsicht- und unerreichbar. Dazu werden Verschlüsselungs- und Anonymisierungsdienste wie TOR oder I2P genutzt. Ohne diese Zugänge (und das Wissen um die damit erreichbaren Dienste) sind entsprechende Angebote unsichtbar.

Der deutsche U(ntergrund)-Markt beziehungsweise Schwarzmarkt ist primär als DeepWeb-Angebot zu klassifizieren. Das heißt, die entsprechenden Foren und Marktplätze findet man in der Regel nicht „einfach so" via Suchmaschine. Allerdings kann man diese, sofern man die Adressen kennt, über einen normalen Webbrowser erreichen und, nach Anmeldung, deren Inhalte auch durchforsten. Dies gilt im Übrigen zum Beispiel auch für Angebote im russischen Untergrund.

Eine Besonderheit beim deutschen Untergrund ist aber, dass viele Seiten optional auch über Darknet-Dienste, insbesondere TOR, erreichbar sind. Das heißt, diese Dienste sind zwar „normal" erreichbar – für Interessenten, die sich aber anonym und nicht nachvollziehbar (zum Beispiel für Strafverfolgungsbehörden) bewegen wollen, sind diese Angebote auch via Darknet erreichbar.

Welche Rolle spielt „The Onion Router" (TOR) in den dunklen und kriminellen Seiten des Internets?

Neben „Invisible Internet Project" (I2P) stellt TOR einen der bekanntesten und am meisten verbreiteten Mechanismen dar, um anonym und verschlüsselt auf (anders nicht erreichbare) Dienste zuzugreifen. Richtig genutzt, sind sowohl die Kommunikation sicher als auch Nutzer und Dienst anonym und nicht nachverfolgbar. Dies macht TOR unter anderem für Dissidenten oder Whistleblower interessant, deren Leben unter anderem davon abhängt, anonym und nicht nachvollziehbar zu kommunizieren.

Leider ist diese Kommunikation aber auch für Kriminelle interessant, die damit der Strafverfolgung entgehen wollen. Mithilfe von TOR können im Darknet auch kriminelle Dienste oder verbotene Waren gehandelt werden – und zwar so, dass sowohl Käufer als auch Anbieter nur schwer zu bestimmen sind.

Macht man sich verdächtig, wenn man aus ganz legalem Anonymitätsbedürfnis heraus TOR im Netz nutzt? Oder ist das sowieso gefährlich?

Einen „Generalverdacht" gegen TOR-Nutzer gibt es zumindest in unserem Rechtsraum nicht. Aufgrund der Funktionsweise von TOR kann es aber durchaus passieren, dass Strafverfolgungsbehörden im Rahmen von Ermittlungen einen bestimmten TOR-Knoten überwachen. Kommuniziert man nun auch (zufällig) über diesen Knoten, „kann" die Kommunikation (bzw. entsprechende Metadaten) erhoben werden. Dies ist an und für sich nicht gefährlich – eventuell „überwacht", und sei es nur als „Beifang", wird man eventuell schon.

Wie sieht das für Java-Anwendungen mit TOR aus?

Grundsätzlich muss man festhalten, dass eine Anwendung in der Regel TOR explizit unterstützen muss. Nur weil man TOR auf einem PC installiert hat, heißt das noch lange nicht, dass alle Applikationen ab sofort „anonym" genutzt

werden können. Der Support für TOR muss in einer Applikation explizit enthalten sein – Ausnahme ist die Kommunikation über einen SOCKS/TOR-Proxy.

Im Fall von Java besteht also die Option, SOCKS zu konfigurieren – sofern die Anwendung dies zulässt. Alternativ gibt es für Java auch Bibliotheken, die es Applikationen erlauben, direkt TOR zu nutzen (z. B. „Orchid“, `https://subgraph.com/orchid/index.en.html`). Dieser Weg ist aus Sicherheitssicht definitiv vorzuziehen. Die bewusste Entscheidung eines Entwicklers, TOR zu unterstützen, bewirkt in der Regel auch, dass dieser sich weitere Gedanken über die übertragenen Daten macht.

Benutzt man eine Applikation über einen TOR-Proxy, ist es eher „suboptimal“, wenn die Applikation in der Kommunikation zum Beispiel Daten überträgt, die wieder Rückschlüsse auf den Nutzer zulassen. Bestes Beispiel ist die Nutzung „normaler“ HTTP-Bibliotheken, die in jedem HTTP-Request fein säuberlich das Betriebssystem, Java-Version, Hostname usw. als HTTP-Header übertragen. Da hilft dann auch TOR nicht mehr.

Bindet ein Entwickler TOR explizit ein, ist zumindest die Chance größer, dass er ähnliche „Lecks“ schließt oder gar nicht erst entstehen lässt. Im einfachsten Fall aktiviert man bei entsprechenden Kommunikations-Bibliotheken im Debug-Build die Ausgabe der Requests/Responses. Tauchen dort dann Daten auf, die Rückschlüsse auf den Benutzer, Geolokation, Provider usw. zulassen, gilt es, diese „Leaks“ im Code zu adressieren.

Woran merken Unternehmen, dass sich Cyberkriminelle in ihrer IT einnisten?

Mittels „Überwachung/Monitoring“ beziehungsweise „Integrität“ – heutige Umgebungen liefern (tief versteckt) in den Unmengen an Log-Daten häufig genug Hinweise, dass zumindest „was faul“ ist. Ist der Initialverdacht geweckt, geht dann die echte Suche los. Leider stellen die Unmengen an Log-Informationen viele vor ein ganz eigenes Problem. Kein Mensch kann diese in der Regel noch manuell durchschauen. Hier sind also Lösungen gefragt, die Log-Daten aus- und bewerten. In diesem Kontext haben sich SIEM-Systeme (Sicherheitsinformations- und Ereignis-Management) in den letzten Jahren durchaus bewährt. Allerdings sind diese Systeme nur so gut wie die Log-Daten, mit denen man diese „füttert“.

Log-Daten sind aber häufig die ersten „Ziele“, die ein Angriff verwischt und damit das SIEM „blendet“. Daher setzen sich inzwischen vermehrt sogenannte „Breach Detection Systeme“ durch, die mittels vielfältiger Techniken wie Netzwerküberwachung, Sandboxing und Verhaltensanalyse unabhängig vom normalen Logging Daten erheben und auswerten. Füttert man diese Daten in ein SIEM, erhöht sich die Qualität natürlich immens. Hinzu kommt, dass die dabei erhobenen Rohdaten auch im Nachhinein die forensische Untersuchung darüber, „was eigentlich passiert ist“, massiv erleichtern.

Eine Alternative beziehungsweise Ergänzung ist das Prüfen der Integrität. Bei vielen heute im Einsatz befindlichen Systemen gibt es, außer den Änderungen an Daten(-banken), keinen sinnvollen Grund, Systemeinstellungen in Produktion zu ändern. Bevor ein System also in Produktion geht, wird ein Abbild des Systems erstellt. Dieses Abbild wird regelmäßig mit dem System verglichen. Gibt es dort Abweichungen, so ist dies zumindest eine Prüfung wert.

Kann es sein, dass man auf der Suche nach Sicherheit im Netz versehentlich bei „secunet.cc“ landet und dort auf ein ganz anderes als das erwartete Szenario trifft?

Wenn man sich für Cybersicherheit interessiert, kann es durchaus passieren, dass man auch auf entsprechende Untergrundforen trifft. Einige dieser Foren bieten in bestimmten Bereichen auch durchaus legale Diskussionen zu IT-(Sicherheits-)Themen an. Ob dies nun einfach so „geduldet“ wird oder eine bewusste Entscheidung ist, um sich zu „tarnen“, sei einmal dahingestellt. Gerade für neue Benutzer ist der kriminelle Teil oft nicht auf den ersten Blick ersichtlich. Als „Neuling“ besitzt man oft gar nicht die Rechte, um die eigentlich kriminellen „Bretter“ und Diskussionen zu sehen. Erfahrungsgemäß kann man trotzdem oft feststellen, dass man in dunkle Bereiche vordringt. Und sei es zum Beispiel bei den Kommentaren zu Sicherheitslücken oder Breaches, wo auf den Opfern auch noch herumgehackt wird!

Woran merken Entwickler, dass ihr Know-how „Made in Germany“ gegen Bezahlung für illegale Webanwendungen missbraucht werden soll?

Hierauf gibt es keine pauschale Antwort – insbesondere, da geforderte Entwicklungen oft gar keinen direkt sichtbaren Bezug zu kriminellen Aktivitäten haben. Allerdings kann man vieles schon mit einem „normalen“ Geschäftsverhalten umgehen, das heißt, bei Beauftragungen zum Beispiel den Auftraggeber prüfen: Wenn dies zum Beispiel augenscheinlich eine Kapitalgesellschaft (GmbH/AG) ist, kann man den Handelsregistereintrag prüfen. Dort stehen dann auch Gesellschafter und/oder Geschäftsführer. Im Zweifelsfall einfach mal anrufen.

Ähnliches gilt für „ordentliche“ Auftragsdokumente (Auftragsgegenstand, Preis, Zahlungsmodalitäten) und Rechnungen. Und natürlich nicht zu vergessen, die eigentliche Bezahlung. Bitcoins oder „Bar-auf-die-Kralle“ müssen zwar nicht negativ sein, sind aber im normalen Geschäftsleben auch nicht die Regel ...

Letztendlich muss man fairerweise aber auch sagen, dass es nur wenige Fälle gibt, in denen „unbescholtene“ Entwickler beauftragt werden. Auch im Untergrund gibt es genügend Entwickler, die sich „anbiedern“. Das heißt, sie erbringen eine Dienstleistung und es ist ihnen letztendlich egal, ob diese kriminell ist oder einen kriminellen Hintergrund hat – solange das Geld stimmt.

Ein anderer Aspekt ist aber Open-Source-Software. In den allermeisten Tools für Cyberkriminelle (Webseiten, Bibliotheken, Samplecode, Executables, Treiber usw.) befinden sich große Mengen an Open-Source-Software. Das heißt, kriminelle Entwickler bedienen sich bei vielen Open-Source-Projekten, um ihre „Machwerke“ zu erstellen. Dies ist für viele Open-Source-Programmierer verständlicherweise befremdlich. Leider lässt sich dagegen wenig machen ...

Wie sollten sich Entwickler verhalten, wenn ihnen ein Auftrag aus dem cyberkriminellen Untergrund angeboten wird, ohne ihre persönliche Sicherheit zu gefährden?

Erfahrungsgemäß reicht ein einfaches „Nein“ – dies ist in der Regel problemlos und gefahrlos möglich. Wenn man nicht gerade die absolute Ausnahme oder Koryphäe auf einem ganz bestimmten Gebiet ist, bleiben für einen potenziellen kriminellen Auftraggeber noch weitere Optionen/Entwickler offen. Aus Sicht des Kriminellen „lohnt“ sich der Aufwand, einen Entwickler zu „überzeugen“, also schlichtweg nicht. Auch hier regiert das Geld ...

Ist man hingegen eine Ausnahme beziehungsweise Koryphäe und der potenzielle Auftraggeber übt Druck aus, bleibt letztendlich nur der Weg zur Polizei. Man muss sich darüber im Klaren sein, dass man es hier oft nicht mit „Kleinkriminellen“ zu tun hat. Die Verbindungen vom Untergrund zur klassischen organisierten Kriminalität sind kurz und gut. Selbst aktiv zu werden, geht kaum – hier hilft dann wirklich nur noch der Gang zur Polizei mit allen Konsequenzen.

Text: Annegret Handel-Kempf (AHK),
Foto: Trend Micro