Inhaltsverzeichnis:

1.	Aktuelle Gefahren/Bedrohungen/Hinweise	Seite 2
1.1	Adobe Flash-Player Zero-Day-Exploits	Seite 2
2.	Darknet – das „dunkle“ Internet	Seite 2
3.	Rückblick auf den Safer Internet Day 2015	Seite 4

1. Aktuelle Gefahren/Bedrohungen/ Hinweise

1.1 Adobe Flash-Player Zero-Day-Exploits

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnte in der jüngeren Vergangenheit vor kritischen Sicherheitslücken im Adobe Flash-Player. Bestimmte Versionen des Wiedergabe-Tools für aktive Inhalte seien anfällig für Angriffe mittels Exploit-Kits, in deren Folge möglicherweise externe Personen Zugriff und Kontrolle über infizierte Systeme erlangen könnten. Das BSI rät daher zur Deaktivierung des Flash-Players bzw. zur Versionsprüfung und schnellstmöglichen Installation der Adobe-Sicherheits-Updates. Betroffene Versionen finden sich aktuell unter:
https://www.buerger-cert.de/archive?type=widtechnicalwarning&nr=TW-T15-0006%20UPDATE%201

2. Darknet – das „dunkle“ Internet

Das Internet mit seinen Möglichkeiten und Risiken hat sich zu dem Massenmedium überhaupt entwickelt: Browser, E-Mail, Suchmaschinen und Soziale Netzwerke werden selbstverständlich genutzt insbesondere von jungen Menschen, den sogenannten „Digital Natives“. Die Gefahren und Risiken der Internetnutzung sind allgegenwärtig und auch dank konsequenter Aufklärungs- und Präventionsarbeit im Bewusstsein vieler Nutzer.

Was viele Nutzer jedoch nicht wissen: Das Internet umfasst auch „dunkle“ oder versteckte, nicht mittels normaler Suchmaschinen erschließbare Bereiche, die neue Gefahren, Risiken und Kriminalitätspotenziale bergen. Das sogenannte „Hidden Internet“, auch „Deepweb“ genannt, soll über 90 Prozent des weltweiten Internetinhalts umfassen. Ein Großteil davon sind Datenbanken und passwortgeschützte Mitgliederbereiche meist legaler Natur. Das sogenannte „Darknet“, das nur mittels spezieller Software zugänglich ist, ist ebenfalls Teil des „Hidden Internet“. Zu den bekanntesten Softwareprodukten gehören „The Onion Router“ (TOR), „The Invisible Internet Project” (I2P) und „The Free Network“ (Freenet).

Die sicherheitstechnischen Risiken, die bei jeder Internetnutzung bestehen, dürfen auch bei einem Ausflug ins Darknet nicht außer Acht gelassen werden. Vielmehr können sich die Risiken insbesondere für unerfahrene Nutzer im Darknet noch erhöhen. Am häufigsten wird Malware aus unsicheren Quellen über das „dunkle“ Netz verbreitet. Aber Kriminelle ködern und betrügen im Darknet vor allem unerfahrene Neulinge. Darüber hinaus besteht durch die Dichte an kriminellen Inhalten, die Unübersichtlichkeit der Netze und die fehlende Kontrolle jederzeit die Gefahr, sich ungewollt in einer Grauzone zwischen legal und illegal zu bewegen.

Tipps der Polizei
Die Polizeiliche Kriminalprävention rät daher Nutzern auch im Darknet besonders auf die bereits bekannten und kommunizierten Vorsichtsmaßnahmen zu achten und aufmerksam zu sein.

- Vertrauen Sie keinen unbekannten Quellen.
- Lassen Sie sich nicht von scheinbar unschlagbaren Angeboten ködern, die Sie so im freien Internet nicht finden würden.
- Achten Sie auf die Aktivitäten Ihrer

Kinder im Internet. Möglicherweise haben sie das Darknet bereits für sich entdeckt. Dann gilt es auf die Gefahren und Risiken hinzuweisen bzw. abzuwägen, ob eine Nutzung wirklich notwendig ist.

Hintergrundinformationen über das Darknet

Technisch betrachtet ist ein Darknet eine Variante eines Virtual Private Networks (VPN), also eines gerouteten abgeschlossenen IP-Raumes, der nicht mit einem normalen Browser zugänglich ist. Am Beispiel des TOR-Netzwerkes lässt sich die Funktionsweise dieser Netze leicht erklären.

Das populäre kryptierte TOR-Netzwerk basiert auf der TOR-Technologie. Zur anonymen Gestaltung der Kommunikation wird ein System von weltweit verteilten Servern genutzt, um den Weg einer Kommunikation so zu verschleiern, dass diese nicht mehr oder nur sehr schwer zurück zu verfolgen ist. Namensgeber für die Technologie ist auch das Zwiebelprinzip: Dabei werden Datenpakete „schichtweise" durch weltweite Knotenpunkte auf Servern transportiert. Diese Technologie ermöglicht es auch, sich Zugang zu den abgeschlossenen Bereichen des Darknets zu verschaffen und verschlüsselte Datenpakete durch das Netz zu schicken. Zugangsvoraussetzung ist lediglich, dass systemabhängig der jeweilige TOR-Browser oder das entsprechende Plug-In installiert wird.

Die Navigation im Darknet ist allerdings nicht so komfortabel wie im „offenen" Internet. Klar aufgelöste Domains sucht man derzeit noch vergebens, wenn auch neue spezielle Suchmaschinen wie GRAMS die Navigation erleichtern und die Hürde bei der Nutzung der versteckten Netze weiter herabsetzen. Die sogenannten Hidden Services der Darknets, also die versteckten Inhalte und Angebote, erschließt sich der Nutzer derzeit noch über eine Art Inhaltsverzeichniss, wie z. B. „The Hidden Wiki". Es handelt sich dabei um ein inoffizielles Eingangsportal, von dem aus durch Weiterklicken die gesuchten Inhalte erschlossen werden können. Diese lassen sich aber auch über eine gezielte URL-Suche im „offenen" Internet finden.

Die Darknets sind mittlerweile zu gigantischen Marktplätzen für illegale Güter und Dienstleistungen aller Art mutiert. Mit den versteckten anonymen Netzen entstanden Webshops für Betäubungsmittel, Waffen, gefälschte Dokumente und Zahlungsmittel oder auch gestohlene Kreditkartendaten und Identitäten. Darüber hinaus lassen sich in der dortigen Underground Economy modularisierte Angriffstools von Hackern oder Malware jeder Art – also der individuell angepasste Cyberangriff – kaufen. Außerdem dienen diese Netze auch dem anonymen File-Sharing von geschützten oder verbotenen Medien, wie z. B. Kinderpornografie.

Die Bezahlung auf diesen Plattformen erfolgt meist mittels virtueller Währungen wie beispielsweise „Bitcoin". Auf diese Weise kann die Anonymität der Beteiligten auch im Zahlungsprozess erhalten bleiben. Hintergrund ist, dass auch Zahlungsströme virtueller Währungen nur schwer nachvollziehbar und zurück verfolgbar sind, da keine regulären Banken in den Zahlungsverkehr eingebunden sind.

Die Darknets dienen jedoch nicht per se nur kriminellen Nutzern zur Verschleierung ihrer Aktivitäten. Nicht alles, was angeboten wird, ist illegal. Es sollte auch

nicht unerwähnt bleiben, dass die abgeschlossenen Netze in manchen Staaten der Welt die letzte Möglichkeit freier Meinungsäußerung sind, da dort eine kritische, nicht-anonyme Kommunikation schwere Strafen zur Folge haben kann. Darknets haben daher durchaus ihre Daseinsberechtigung.

Quellen:

Ries, U., Erster Einstieg ins Hidden Web, http://www.chip.de/artikel/Darknet-Das-Tor-ins-Deep-Web-6_63227355.html (Stand: 24.02.15)

Potts, C., In den Abgründen des Internets, http://www.handelsblatt.com/technik/it-internet/cebit2014/deep-web-in-den-abgruenden-des-internets/9599476.html (Stand: 24.02.15)

Rouse, M., Definition Darknet, http://www.searchsecurity.de/definition/Darknet (Stand: 24.02.15)

Schiffer, C., Expedition ins Darknet, http://www.br.de/radio/bayern2/kultur/radiofeature/expedition-im-darknet-100.html (Stand: 24.02.15)

Taiber, R., Wie komme ich in das Darknet?, http://www.taiber-unternehmensberatung.de/darknet-zugang-darknet-tor-nutzen/ (Stand: 24.02.15)

Neon Redaktion, Der Weg ins Darknet, http://blog.neon.de/2013/11/der-weg-ins-darknet (Stand: 24.02.15)

3. Rückblick auf den Safer Internet Day 2015

„Gemeinsam für ein besseres Internet“ („Let's create a better internet together“) lautete das Motto des diesjährigen Safer Internet Day (SID), der europaweit am 10. Februar 2015 stattfand. Die Europäische Kommission als Initiator dieses seit 2004 durchgeführten Aktionstages will damit u.a. die Sensibilität für das Thema „Sicheres Internet“ fördern, die öffentliche und mediale Aufmerksamkeit auf das Thema „Sicheres Internet" lenken und letztlich Menschen aller Altersgruppen dazu bewegen, der Sicherheit im Internet mehr Aufmerksamkeit zu schenken.
Teilnehmen am SID können alle, die Interesse am Thema haben und etwas beitragen möchten (Unternehmen, Schulen, Jugendorganisationen, Bildungseinrichtungen, Vereine, Privatpersonen etc.) In Deutschland initiiert und koordiniert klicksafe (www.klicksafe.de), eine Sensibilisierungskampagne zur Förderung der Medienkompetenz im Umgang mit dem Internet und Neuen Medien im Auftrag der Europäischen Kommission, alle Aktionen und Veranstaltungen zum SID.

Wer sich dafür interessiert, welche Aktionen in seiner Nähe durchgeführt wurden, der kann sich auf einer Deutschlandkarte alle Veranstaltungen anzeigen lassen, die klicksafe über das Registrierungsformular gemeldet wurden: http://www.klicksafe.de/ueber-klicksafe/safer-internet-day/sid-2015/google-maps-karte-sid-2015/.
In einer weiteren Übersicht (http://www.klicksafe.de/ueber-klicksafe/safer-internet-day/sid-2015/sid-veranstaltungen-2015/ können sich Interessierte zudem eine Liste mit allen Veranstaltungen anzeigen lassen, die klicksafe gemeldet wurden.

Das Programm Polizeiliche Kriminalprävention (ProPK) hat im Zusammenhang mit dem Safer Internet Day seine Filme und Broschüren rund um das Thema „Mediensicherheit“ beworben:

„Klicks-Momente“ für Internetnutzer:
http://www.gsbl.extrapol.de/propkmedienportal/index.php?option=com_fabrik&c=form&view=details&Itemid=2&fabrik=2&rowid=196&tableid=2&fabrik_cursor=8

„Klicks-Momente“ für Eltern und Erziehungsverantwortliche:
http://www.gsbl.extrapol.de/propkmedienportal/index.php?option=com_fabrik&c=form&view=details&Itemid=2&fabrik=2&rowid=209&tableid=2&fabrik_cursor=7

Medienpaket „Verklickt!“:
http://www.gsbl.extrapol.de/propkmedienportal/index.php?option=com_fabrik&c=form&view=details&Itemid=2&fabrik=2&rowid=208&tableid=2&fabrik_cursor=10

Sicherheitskompass:
http://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/sicherheitskompass.html

Weitere Medien erhalten Sie im ProPK-Medienportal unter: http://www.gsbl.extrapol.de/propkmedienportal/