25. Mrz. 2015

von Martin

in Cyber Security, Sicherheitskultur, Terrorismus

Kommentare (4)

Zwischen Paranoia und Propaganda: Jihadistische Gruppierungen und ihre IT-Sicherheit

von Martin Schmetz

Teil XXI unserer Serie zum „Islamischen Staat“

Islamistische Terrorgruppen setzen in mehrfacher Hinsicht auf das Internet. Für islamistische Gruppierungen wie Al Qaida oder den islamischen Staat stellen eigene Foren und Webseiten, Instant Messenger wie Kik oder WhatsApp sowie soziale Medien wie Twitter, Facebook oder Ask.fm eine wichtige Plattform für Propaganda, Rekrutierung sowie Organisation und Logistik dar. Auf diese Infrastruktur zu verzichten würde den Verzicht auf ein extrem mächtiges Werkzeug bedeuten. Auf der anderen Seite ermöglicht die Nutzung dieser Dienste auch die leichtere Überwachung durch Geheimdienste. Auf diesen Zwiespalt haben islamistische Gruppierungen mit unterschiedlichen Strategien reagiert. Wie lösen der Islamische Staat und al-Qaida diese Spannung auf? Und was bedeutet dies für westliche Staaten? In diesem Post soll darauf eingegangen werden.

Es sei darauf hingewiesen, dass einige Links direkt auf Anleitungen und Texte von Untersützern jihadistischer Terrororganisationen verweisen. Wer sich unwohl dabei fühlt, sollte bitte Vorsicht bei Klick auf Links walten lassen.

Propaganda und Kommunikation

Andere Autoren in der Beitragsreihe haben bereits darauf hingewiesen, dass soziale Medien ein wichtiges Werkzeug für islamistische Gruppierungen sind um Propaganda zu betreiben und Nachwuchs zu rekrutieren. Es erscheint daher paradox, dass die meisten Anleitungen von Jihadisten im Netz zum Schutz vor Geheimdiensten von der Nutzung sozialer Netzwerke abraten. Weil ein vollständiger Verzicht auf diese Medien mit zu hohen Kosten einhergeht, wird zähneknirschend meist als Alternative empfohlen, ein komplett neues Profil zu eröffnen, dass sich mit jihadistischen Themen befasst, aber keinerlei Rückschlüsse auf den Autor zulässt. Dieses soll nur über ein VPN oder Tor verwendet werden, wobei gerade letzteres möglicherweise eine riskante Strategie ist. Hat man auf seinem privaten Profil bereits entsprechende Datenspuren hinterlassen, rät eine Anleitung zudem dazu, einen Hinweistext zu hinterlassen, der nahelegt, dass man sich von jeglicher Form von islamistischer Gewalt distanziert und sich lediglich aus akademischen Gründen mit diesen Themen auseinandergesetzt hat.

Brand Marketing vs. OPSEC

Für weniger öffentliche Kommunikation macht die Verwendung von Verschlüsselung Sinn. Diese spielt aber erst in größerem Maße seit den Snowden-Enthüllungen eine Rolle: Inzwischen wird etwa bei den einschlägigen Jihadisten-Magazinen wie Inspire neben der Mailadresse auch ein Schlüssel angegeben, um verschlüsselten E-Mailverkehr zu ermöglichen. Allerdings setzt man dabei nicht auf bereits etablierte Software, sondern hat

SOCIAL MEDIA

SUCHE

Suche...

Suche

TWITTER FEED

Diana Schubert über die Rolle von #Kommunen in der #Prävention von #Radikalisierung https://t.co/6F0QGmsxoQ #Salafismus
about 5 hours ago from Twitter Web Client

Fördern die Medien #Salafisten? Dynamiken, Verantwortung & Grenzen der Berichterstattung über salafistische Gruppen https://t.co/YM8phOlqdf
25. Januar 2016, 9:14 from Twitter Web Client

Riem Spielhaus fragt heute: Brauchen wir eigentlich wirklich mehr Forschung zum #Salafismus? Und wenn ja: welche? https://t.co/9DFU0rg0PE
21. Januar 2016, 9:28 from Twitter Web Client

TAGS

BELIEBT KOMMENTARE NEU

"Die Flüchtlinge", "die Rassisten" und "Wir" – zu den Ambivalenzen

eigene entwickelt (die allerdings auf standardisierte Algorithmen und Bibliotheken setzt). Das ist eine durchaus fragwürdige Strategie, denn kryptographische Algorithmen halbwegs bugfrei zu implementieren ist keineswegs einfach. Zudem ist die Nutzung weit verbreiteter Verschlüsselungsprogramme wie PGP unverdächtig. Wer hingegen Software aus der Jihadistenszene verwendet, dürfte ziemlich sicher für Geheimdienste interessant sein. Und es ist keinesfalls unmöglich an die Daten der Verwendung dieser Software zu kommen: Jeder Virenscan etwa könnte dies leicht erfassen, so das Interesse auf Seiten der Virenscannerhersteller daran besteht.

Es steht daher zu vermuten, dass die Verwendung eigener Software vor allem PR-Aspekten dient. Verbreitete Verschlüsselungsprogramme sind open source und somit unverdächtig und die Programme der Jihadisten verwenden die gleichen Algorithmen. Wollte man möglichst unverdächtig und sicher kommunizieren, würde man also auf open source Software setzen. Dies stellt aber aus Marketingsicht keinen Gewinn dar. Diese Vermutung wird gestärkt durch die Tatsache, dass sowohl al-Qaida als auch der Islamische Staat tatsächlich sensitive Daten nur selten über das Internet verschicken. Stattdessen werden Kuriere mit USB-Sticks eingesetzt, die Daten von nicht ans Internet angeschlossenen Rechnern zu anderen nicht ans Internet angeschlossenen Rechnern transportieren.

Gerade letzteres zeigt auch, dass die elektronische Überwachung der islamistischen Terrorszene im Netz wohl nur selten tatsächlich brauchbare Informationen über die wirklich sensitiven Operationen dieser Gruppen gibt. Diese Daten werden nicht über das Internet transportiert. Da sie auch keinen direkten Propagandawert haben, entziehen sich die Akteure so auch dem Widerspruch zwischen Öffentlichkeitswirksamkeit und OPSEC. Es ist aber der wichtige größere Unterstützerkreis, der diese Gruppierungen angreifbar macht. Denn über Propaganda in sozialen Netzwerken, Foren und auf Webseiten machen sie sich außerhalb der Krisenregionen bekannt, können ihre eigene Narrative verbreiten, finanzielle Unterstützung einsammeln und Personen im Westen rekrutieren. Dies geschieht aber über Dienste, die von westlichen Firmen betrieben werden und somit überwachbares Terrain darstellen.

Gute und schlechte Tipps

Bisher scheinen jihadistische Akteure darauf keine sinnvolle Antwort gefunden zu haben: Zwar können E-Mails und Chats verschlüsselt werden (so denn tatsächlich sichere Software und Dienste eingesetzt werden), aber dies schützt weder vor infizierten Rechnern noch eignet sich dies für breitere Propaganda. Ein Ausweichen auf eigene Plattformen würde gleichzeitig aber das Ende des breiten Publikums bedeuten. Twitter und Facebook werden aus gutem Grund benutzt – jeder kennt und nutzt diese Webseiten. Es bleibt also nur der Versuch eines halbwegs anonymen Zugriffs auf diese Dienste. Dies stellt aber zum einen für die meisten Nutzer eine fast unüberwindbare Hürde auf Grund der technischen Komplexität dar, außerdem nimmt dies bugfreie, sichere Software und korrekte Bedienung in 100% der Fälle an.

Jihadisten haben daher ähnliche Probleme mit IT-Sicherheit wie Unternehmen: Die meisten Nutzer haben weder die Kenntnisse noch die Disziplin, die entsprechenden Konzepte sinnvoll umzusetzen, geschweige denn einen gezielten Angriff zu erkennen. Der Islamische Staat etwa hat, genau wie viele Unternehmen, erheblich mit dem Phänomen BYOD (Bring Your Own Device) zu kämpfen: Gerade aus dem Westen zugereiste Jihadisten benutzen weiterhin ihre mitgebrachten Smartphones oder Computer. Sie machen sich beispielsweise bei Uploads auf Facebook oder Twitter keine Gedanken über etwa in Bildern eingebetteten Metadaten. Die

im aktuellen Flüchtlingsdiskurs

Ich bin Paris! Ich bin Muslim! Ich bin Nato? Die offene Gesellschaft und ihre Feinde nach dem 13. November.

Der Dschihad der Auslandskämpfer: Ausdruck einer Subkultur

Terroristen oder Bürgerkriegsflüchtlinge? Was wir gegen diese Verwechslung tun müssen

Syria's Present Anticipates A Future Sunni-Flavoured Iran

KATEGORIEN

Außenpolitik (64)
Bürgerkriege (24)
Cyber Security (52)
Demokratisierung (14)
Drohnen (15)
Flüchtlinge (17)
Humanitäre Interventionen (15)
Innere Sicherheit (32)
Interviews (10)
Katastrophen (4)
Konferenz (29)
Militär (31)
Pandemien (2)
Podcast (7)
Popkultur (22)
Raketenabwehr (1)
Sanktionen (8)
Security Culture (27)
Sicherheits-Kommunikation (16)
Sicherheitskultur (237)
Sozialwissenschaft Online (71)
Stellenangebote (55)
Strategie (12)
Terrorismus (60)
Theorie (5)
Umwelt (1)

darin enthaltenen Ortsdaten wurden aber bereits für Drohnen- und Bombenangriffe genutzt. In Anleitungen verbietet daher der Islamische Staat zugereisten Jihadisten inzwischen die Nutzung von iPhones, die als besonders anfällig für Überwachung angesehen werden, und rät generell dazu, die Telefone in Alufolie einzuwickeln, so sie überhaupt betrieben werden sollen.

Der Tipp, Geräte in Alufolie einzuwickeln ist symptomatisch für ein weiteres Problem vieler Anleitungen, die in einschlägigen Foren und auf Twitter und Facebook zirkuliert werden: Sie enthalten neben sinnvollen Hinweisen auch viel sinnloses oder sogar kontraproduktives und für Laien ist es nur schwer möglich, zwischen guten und schlechten Tipps zu unterscheiden. Auf absehbare Zeit sieht es daher so aus, als ob das Internet für islamistische Terrorgruppen wie den Islamischen Staat oder Al Qaida ein zwiespältiges Angebot bleibt: Ohne geht es nicht, denn es bleibt dann gerade der mediale Erfolg im Westen aus. Aber mit geht es eigentlich erst recht nicht, denn dies ermöglicht auch die leichte Überwachung durch westliche Geheimdienste und sät Zweifel und Unsicherheit im Unterstützerkreis.

Tags: al-Qaida, cyber sicherheit, Islamischer Staat, it-sicherheit, Terrorismus, Überwachung

« CfP zur interdisziplinären Konferenz des Forums Privatheit: Die Zukunft der informationellen Selbstbestimmung

Stellenanzeigen März 2/2 »

4 Kommentare zu “Zwischen Paranoia und Propaganda: Jihadistische Gruppierungen und ihre IT-Sicherheit”

Janusz | 29. Mrz. 2015 um 16:54 | **#1**

Eine andere beliebte Technik zur Kommunikation unter Dschihadisten – beschrieben bspw. durch Morten Storm am Bsp. AQAP and Awlaki – ist die Kommunikation mittels E-Mail-Entwürfen in geteilten E-Mail-Postfächern. Wurde dies auch in IS-Magazinen o.ä. beworben? Wie wird dem von Sicherheitsbehörden begegnet?

ANTWORTEN

Martin | 30. Mrz. 2015 um 8:14 | **#2**

Interessanterweise habe ich davon in den entsprechenden Anleitungen nichts gelesen. Wieso dem so ist kann ich aber auch nicht sagen. Möglicherweise weil diese Kommunikationsweise nicht verschlüsselt ist. Und für Anleitungen die sich mit sicherer Twitter Nutzung o.ä. beschäftigen ist das natürlich keine Alternative, da dort kein breiteres Publikum besteht.
Mir wäre auch von Strafverfolgungsseite keine Strategie dagegen bekannt, aber das verwundert mich weniger. Das würde sehr konkret etwas über die Überwachungsfähigkeiten von Webmail Diensten aussagen, ich glaube nicht, dass daran Interesse besteht. Allerdings werden Entwürfe ebenso analysiert für Werbung etc, sollte automatisiert gesucht werden würden die ebenso erfasst. Hinzu kommt dass viele Anbieter sowieso Alarm schlagen wenn logins aus unterschiedlichen Ländern ins gleiche Postfach erfolgen. Das wäre sicherlich ein Ansatzpunkt für eine detaillierte Analyse des Postfachs.

ANTWORTEN

Versicherheitlichung (23)
Visualisierung (6)
Whistleblowing (8)
WikiLeaks (17)
WMD (10)
Zivilgesellschaft (66)

BLOGROLL

Arbeitskreis soziale Bewegungen
Augen geradaus
Dan Drezner
Dart-Throwing Chimp
David Campbell
de.hypotheses.org
Demokratieforschung Göttingen
Duck Of Minerva
Future and Politics
Hylaean Flow
Internet und Politik
IR Blog
Just Security Blog
justsecurity.org
Killer Apps
Kings Of War
MPC Journal – Muslim Politics and Culture
netzpolitik.org
percepticon
shabka.org
Terrorismus in Deutschland
theorieblog.de
Verfassungsblog
Vom Bohren harter Bretter
whistleblower-net.de

ARCHIV

Wähle den Monat

Trackbacks/Pingbacks

1. **Sich informieren V | schneeschmelze | texte** - 31. Mrz. 2015

   [...] des Lehrstuhls, teils Mitarbeiter der Hessischen Stiftung Friedens- und Konfliktforschung. Dort liest man unter anderem, daß Jihadisten „Kuriere mit USB-Sticks„ einsetzten, „die Daten von nicht ans [...]

2. **Terror und Medien: Der Cyber-Angriff auf den Sender „TV5 Monde“ durch den IS** - 14. Apr. 2015

   [...] in ähnlicher Weise die terroristischen Organisationen selbst. Martin Schmetz schreibt für den Sicherheitspolitik-Blog der Universität Frankfurt am Main über die Strategien der Dschihadisten, ihre eigene [...]

Einen Kommentar hinterlassen

Name

Email

Webseite

Kommentar