> Von: HERNDLER Christian
> Gesendet: Mittwoch, 26. März 2008 11:54
> Betreff: Ihr Artikel "Konstruktion und Dekonstruktion eines Terroristen"
>
>
> Sg. Hr. Zeger,
>
> Ich habe soeben die Lektüre Ihres Artikels "Konstruktion und Dekonstruktion eines Terroristen ?" beendet und möchte Ihnen diesbezüglich einige Anmerkungen übermitteln.
>
> Abschnitt: "Ergebnisse der technischen Überwachung"
>
> ...wurden bloß lückenhafte Datentrümmer zusammengetragen, die nur in der Masse nicht aber im Inhalt beeindrucken und einer nüchternen Beurteilung nicht standhalten.
>
> Soweit mir bekannt ist wurden die sichergestellten Daten (sowohl jene der Internetüberwachung als auch die Sicherung der Datenträger) zu keinem Zeitpunkt von nicht mit den Ermittlungen beauftragten Personen ausgewertet bzw. beurteilt (es gab keinen Auftrag des Gerichtes die Daten an die Verteidigung auszufolgen), es ist daher rätselhaft wie Sie ohne Kenntnis der Daten diese Aussage tätigen können.
>
> ... Wobei die geringen IT-Kenntnisse des Angeklagten den Überwachern entgegenkamen.
>
> Der Angeklagte hat nicht nur immer wieder seine Fachkenntnisse betont, auch seine Verhaltensweise bei der Nutzung des Computers zeigt deutlich, daß er - wenn er auch keinesfalls als IT-Spezialist zu bezeichnen ist - über wesentlich umfangreichere Kenntnisse im Umgang mit IT-Technik verfügt als der überwiegende Teil der Computernutzer.
>
> ...Geschaffen wurden Plausibilitätsketten, wie etwa folgende: Im Drohvideo werden Bilder verwendet, die auf einer regierungsamtlichen Seite vorhanden sind. Auf diese Seite wurde ein Monat vor der Videoveröffentlichung über einen malaysischen Proxyserver zugegriffen und der Angeklagte hatte auch irgendwann diesen Server benutzt. Also muss der Angeklagte, so der kurze Schluss, etwas mit dem Drohvideo zu tun haben.
>
> Der Angeklagte hatte nicht "irgendwann" diesen Server benutzt, wie im Prozess ausgeführt hat er etwa 1/3 seiner Internetkommunikationen über diesen Server abgewickelt. Darüber hinaus handelt es sich bei diesem Server nicht um einen allgemein zugänglichen anonymen Proxy, dieser Server ist nur nach Authentifizerung mittels Username und Passwort zugänglich.
>
> ...zeitlichen Abläufe genauer darzustellen und so zumindest die Faktenlage zu verbessern. Von wem und in welchem Ausmaß der malaysische Server tatsächlich genutzt wurde, wurde gar nicht versucht darzustellen.
>
> Bei dieser Bemerkung wäre es nur korrekt hinzuzufügen, daß es mit hoher Wahrscheinlichkeit nicht möglich ist, den Nutzerkreis eines Anonymisierungsservers im Ausland zu ermitteln, es liegt schließlich im Wesen eines solchen Servers genau dies zu verhindern.
>
> ...Von den Ermittlungsbeamten wurden dutzende Alias- und Nicknames und Mailadressen präsentiert, wie sie üblicherweise in Foren und Chats verwendet werden. Auch eine Fülle von Dialogen und Beiträgen wurden aufgezeichnet. Hinter diesen Beiträgen stehen zahllose IP-Adressen. Wenn die GIMF tatsächlich eine unternehmensartige Organisation wäre, dann müssten auf Grund dieser IP-Adressen auch Personen identifizierbar sein, die hinter diesen Adressen stehen und die Kontakt mit den Angeklagten hatten.

>
> Ein wesentlicher Teil der Kommunikation betrifft Chats (vor allem unter Nutzung des MSN-Messengers). Bei dieser Anwendung melden sich die Chat-Teilnehmer an einem zentralen Server an (hier einem Server von Microsoft). Da die Kommunikation fast ausschließlich über diese zentralen Server erfolgt kann bei der Überwachung auch lediglich die IP-Adresse dieses Servers aufgezeichnet werden. Eine Zuordnung der einzelnen Teilnehmer kann daher nur zu Nicknamen bzw. Email-Adressen erfolgen. Dabei werden fast auschließlich "Wegwerf-EMailadresse" verwendet, die die Identifizierung wesentlich erschweren bzw. praktisch unmöglich machen.
>
> Abschnitt: "Grosse Chance vertan"
>
> ...Dazu wäre es aber notwendig gewesen einerseits alle technischen Zweifel an der Richtigkeit und Vollständigkeit der Aufzeichnungen zu beseitigen und andererseits die Sachbeweise so verständlich aufzubereiten, dass sie auch objektiv und ohne Kommentar der BVT-Beamten für Berufs- und Laienrichter aussagekräftig sind.
>
> Es wurden zu keinem Zeitpunkt konkrete technische Zweifel geäußert, die sehr allgemein gestellten technischen Fragen wurden beantwortet. Die Aufbereitung komplexer technischer Zusammenhänge auf eine Weise daß sie auch von den Berufs- und Laienrichtern verstanden werden können ist bedauerlicherweise äußerst schwierig, dieses Problem wäre jedoch durch die Beiziehung unabhängiger Sachverständiger lösbar - eine Möglichkeit die von der Verteidigung aus welchem Grund auch immer jedoch nicht wahrgenommen wurde.

>
> ...Unter <ftp://ftp.freenet.at/pri/fragestellungen-gutachter-terrorprozess.pdf> ftp://ftp.freenet.at/pri/fragestellungen-gutachter-terrorprozess.pdf sind einige Fragen zusammengestellt, die sich ein technisch interessierter Prozessbeobachter unwillkürlich stellt
>
> Einige der in diesem Dokument gestellten Fragen hätte ich auch im Prozess erwartet, daß diese nicht gestellt wurden ist jedoch wohl eher ein Problem der Verteidigung. Es kann wohl nicht der ermittelnden Behörde angelastet werden, keine Antworten auf Fragen zu geben die nie gestellt wurden. Sollten Sie jedoch daran interessiert sein kann ich Ihnen anbieten, die in diesem Dokument gestellten Fragen ausführlich zu beantworten (das Einverständnis meiner Vorgesetzten vorausgesetzt).
>
> Abschnitt: "Das Überwachungsniveau der BVT"
>
> ...Wenngleich die informierten Zeugen des BVT und der SEO Auskünfte über die Überwachungsmethoden unter Hinweis auf Ermittlungsschutz verweigerten, ließen sich doch für Experten ausreichend klare Hinweise auf die Methoden finden.
>
> Es wurde zu keinem Zeitpunkt Auskunft über die Überwachungsmethoden des BVT verweigert. Die Art und Weise der Internet-Überwachung wurde detailliert erklärt (in einem der nächsten Absätze beschreiben Sie selbst die Vorgangsweise beim Provider Chello...). Lediglich Auskünfte über das von der SEO verwendete Produkt konnte nicht gegeben werden, es wurde jedoch auch von der SEO die Vorgangsweise und das entsprechende Ergebnis beschrieben.
>
> ...Positiv für die Ermittler war, dass der Angeklagte technisch nur sehr oberflächliche Informatikkenntnisse hatte und neben dem Standard-Betriebssystem "Microsoft Windows XP", auch den "Microsoft Internet Explorer" und "MSN Messenger" verwendete. Für diese Systeme existieren die meisten Überwachungswerkzeuge.
>

> Für die Internet-Überwachung ist es völlig belanglos, welches Betriebssystem bzw. welche Softwareprodukte verwendet werden
>
>   ...Dass bei der forensischen Datensicherung bloß das Disk-Sicherungsprogramm Encase verwendet wurde, das sich etwa zur Integritätssicherung der beschlagnahmten Daten mit dem Hashverfahren MD5 zufrieden gibt, ein Verfahren das seit etwa zehn Jahren als nicht mehr sicher eingestuft wird, ließe Raum für Spekulationen und begründete Vorwürfe, dass Datenmaterial nachträglich manipuliert wurde.
>
> Es entspricht den Tatsachen daß seit einiger Zeit bekannt ist, daß Hash-Kollisionen bei der Verwendung von MD5-Hashes auftreten können. Dabei kann durch genau definierte Veränderungen an bestimmten Stellen des Ausgangsmaterial möglicherweise der gleiche Hash-Wert erzeugt werden - daraus abzuleiten daß MD5-Hashes als Schutz gegen Manipulation nicht mehr ausreicht erscheint jedoch unseriös. Es ist auch derzeit kein anwendbares Verfahren bekannt, wie nach einer Veränderung von Ausgangsmaterial mittels bestimmter, sinnvoller Daten eine Hash-Kollision erzeugt werden kann.
>
>   ...Doch wie formulierte es ein BVT-Beamter in verblüffend naiver Logik: "OpenVPN und Proxyserver, welche Privatperson verwendet das schon, so jemand muss doch was zu verbergen haben!"
>
> Diese Aussage wurde so von mir nie getätigt. Ich habe lediglich zu bedenken gegeben, daß die Verwendung eines VPN und eines Proxyservers (und vor allem die Kombination dieser beiden Dinge) für einen durchschnittlichen Internet-Benutzer eher ungewöhnlich ist. Ich habe darüberhinaus zu keinem Zeitpunkt daraus abgeleitet, daß eine Person durch die Verwendung dieser Dinge automatisch zum Täter wird.
>
>   ...Die Überwachung der eMail-Kommunikation wurde schlicht dadurch unterlaufen dass ein eMail-Account gemeinsam genutzt wurde. Mails wurden nicht verschickt sondern auf einem Mailserver als Mail-Entwurf hinterlegt.
>
> Diese Aussage ist nicht korrekt. Auch um eine Entwurf zu lesen bzw. am Mailserver zu speichern ist die Übertragung der Daten vom und zum Server erforderlich, auch diese Daten werden daher von der Internetüberwachung umfasst.
>
> Zu meinem Bedauern mußte ich bei der Lektüre dieses Artikel feststellen, daß Sie darin in weiten Teilen das tun was Sie an der Vorgangsweise der Behörden kritisieren: Sie stellen technische Details in einer Weise dar die bei einem Laien vielleicht den gewünschten - jedoch keinesfalls einen objektiven - Eindruck von der Vorgangsweise der Behörden hinterläßt. Es spricht nicht für Objektivität eines Autors lediglich jene Details darzustellen die der Sichtweise des Autors entgegenkommen bzw. eigene Interpretationen als Tatsachen darzustellen.
>
> Es besteht kein Zweifel daran daß es sich bei (Internet)Überwachung um ein äußerst komplexes Thema handelt das in Zukunft verstärkte Bedeutung erlangen wird. Ich kann Ihnen jedoch versichern daß auch ich ausschließlich an einer gesetzeskonformen nachvollziehbaren Umsetzung solcher Maßnahmen interessiert bin.
>
> Ich möchte betonen, daß der Inhalt dieser EMail lediglich meine persönliche Meinung darstellt und in keiner Weise als Stellungnahme des BVT zu verstehen ist.
>
> Mit freundlichen Grüßen
>
> Christian Herndler
> +---+
> | Bundesamt für Verfassungsschutz und Terrorismusbekämpfung |

> | Abteilung II/BVT/2 - Technische Ermittlung |
> | Tel.:   +43-1 53126-4320 DW |
> | Mobil: +43 664 414 85 00 |
> | E-Mail: christian.herndler@bmi.gv.at |
> +--+
> | MCSE - Microsoft Certified Systems Engineer/Security |
> | CPTS - Certified Penetration Testing Specialist |
> | EnCE - EnCase Certified Examiner |
> | CHFI - Computer Hacking Forensic Investigator |
> | Network+ Certified / Security+ Certified |
> --+