Threat Update: Man-in-the-Middle Attacks

Lukas Feiler

8. Dezember 2006

Inhalt

1. Einleitung

Anlässlich der vom e-center zum Thema „Sicherheitsfaktor Mitarbeiter“ im Landesgericht für Strafsachen Wien veranstalteten „Security 06“, sollen sog „Man-in-the-middle“ Attacks, wie sie insbesondere von Mitarbeitern, die sich innerhalb des Local Area Networks (LAN) befinden, näher beleuchtet werden. Als Man-in-the-middle Attacks (MITM) werden jene Angriffe bezeichnet, bei denen es dem Angreifer gelingt, sich logisch gesehen zwischen den Kommunikationspartnern zu positionieren. Aus einer derartigen Situation heraus kann der Angreifer einen Denial of Service (DoS) herbeiführen, Sniffing, Phishing oder Hacking betreiben.

2. Eine kleine Einführung in TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) ist eine Sammlung von Protokollen die ebenso im weltweit größten Netzwerk, dem Internet, wie in kleinen privaten Netzwerken zum Einsatz kommt. Eine für die folgenden Ausführungen besonders relevante Frage ist, wie ein Datenpaket von einem System (zB in Wien) zu einem anderen System gelangt, das sich in einem anderen Netzwerk befindet (zB in New York). Die Antwort hierauf ist IP Routing[1]. Insbesondere für Netzwerke kleinerer und mittlerer Größe erfolgt IP Routing durch eine Dezentralisierung der Routing-Informationen. Eine einzelne Workstation kennt idR nur einen einzigen Router, über den alle Datenpakete geleitet werden, die nicht für das lokale Netzwerk bestimmt sind (sog Default Router oder Default Gateway). Erst der Default Router verfügt über weitergehende Informationen wie das Datenpaket an sein Ziel zu gelangen kann.

Innerhalb eines lokalen Netzwerkes stellt sich jedoch die Frage, wie eine Workstation an die Information gelangt, welche IP-Adresse dem zu verwendenden Default Router zugewiesen wurde. Da eine manuelle Konfiguration aller Workstations einen zu großen Arbeitsaufwand verursachen würde, wird häufig DHCP (Dynamic Host Configuration Protocol)[2] zum Einsatz

[1] *Stevens*, 111 ff
[2] spezifiziert in RFC 2131, ftp://ftp.rfc-editor.org/in-notes/rfc2131.txt

gebracht. Eine Workstation sendet nach Aktivierung der Netzwerkkarte (idR währen des Boot-Vorgangs) eine Nachricht an alle Rechner des lokalen Netzwerkes (ein sog Broadcast), um den DHCP-Server ausfindig zu machen. Erreicht der Broadcast einen DHCP-Server, so übermittelt dieser ua die IP-Adressen der Workstation selbst und welche IP-Adresse als Default Router einzutragen ist.

Verfügt die Workstation nun über die IP-Adresse des Default Routers, ist sie grundsätzlich in der Lage, Datenpakete in andere Netzwerke zu versenden. Innerhalb ihres lokalen Netzwerkes, dh jenes Netzwerkes, das aus der Summe aller System besteht, die ohne Zuhilfenahme eines Routers unmittelbar erreichbar sind, ist jedoch noch ein weiteres Protokoll für die Datenübertragung erforderlich: das Address Resolution Protocol (ARP)[3]. Soll innerhalb des lokalen Netzwerkes[4] ein Datenpaket versendet werden, so muss dem sendenden System zunächst die MAC-Adresse (auch Hardware-Adresse oder Ethernet-Adresse genannt) der Netzwerkkarte des Zielsystems bekannt sein. Denn grundsätzlich werden Datenpakete von einem System nur entgegengenommen, wenn die als Ziel eingetragene MAC-Adresse der MAC-Adresse des Systems entspricht.[5] Um die IP-Adresse des Zielsystems in eine MAC-Adresse aufzulösen, wird ein ARP-Request in Form eines Broadcast an alle Systeme des lokalen Netzwerks versendet. Mit dem Broadcast wird das Zielsystem dazu aufgefordert, seine MAC-Adresse bekannt zu geben. Auch um über den Default Router Datenpakete in andere Netzwerke transportieren zu können, ist es erforderlich, dass zunächst mittels ARP die MAC-Adresse des Default-Routers ermittelt wird.

Ein weiteres essentielles Protokoll ist DNS. Es ermöglicht die Auflösung von Domainnamen in IP-Adressen. Dies ist erforderlich, da die Benutzer idR nur den Domainnamen (zB www.example.com) und nicht die IP-Adresse des gewünschten Systems kennen, das Protokoll IP aber die IP-Adresse des Zielsystems benötigt. Jedes System ist grundsätzlich mit zwei DNS-Servern konfiguriert. Die IP-Adressen der zu verwendenden DNS-Server werden häufig per DHCP bezogen. Soll zB der Domainnamen www.example.com in eine IP-Adresse aufgelöst werden, so wird an den primären DNS-Server eine diesbezügliche Anfrage gesendet. Erst nachdem der DNS-Server mit einer IP-Adresse geantwortet hat, kann ein Datenpaket an www.example.com versendet werden.

Somit ergibt sich für das Aufrufen von www.example.com unmittelbar nach dem Starten des Betriebssystems folgender (vereinfachter) Ablauf:

- Zuweisung der IP-Adressen der eigenen Netzwerkkarte, des Default Gateway und der DNS-Server per DHCP.
- Im Browser wird www.example.com eingegeben.
- Um den innerhalb des lokalen Netzwerks befindlichen DNS-Server[6] zu erreichen, muss die bereits bekannte IP-Adresse mittels ARP-Broadcast in die MAC-Adresse des DNS-Servers aufgelöst werden.
- Durch eine Anfrage beim DNS-Server wird www.example.com in eine IP-Adresse aufgelöst.

[3] spezifiziert in RFC 826, ftp://ftp.rfc-editor.org/in-notes/rfc826.txt; vgl *Stevens*, 53 ff

[4] genauer: innerhalb des lokalen Subnets, determiniert durch die Subnetmask (zB 255.255.255.0 bzw /24 in CIDR-Notation); vgl *Stevens*, 140 f

[5] genauer: der MAC-Adresse jener Netzwerkkarte des Systems entspricht, über die das Datenpaket empfangen wurde.

[6] Der DNS-Server könnte sich auch außerhalb des lokalen Netzwerks befinden, diesfalls das Datenpaket über den Default Gateway zu versenden wäre.

- Da die IP-Adresse von www.example.com außerhalb des lokalen Netzwerkes liegt, sind die an www.example.com gerichteten Datenpakete über den Default Router zu versenden.
- Die IP-Adresse des Default Routers ist durch einen ARP-Broadcast in die entsprechende MAC-Adresse aufzulösen.
- Das Datenpaket kann über den Default Router an www.example.com versendet werden.

Im Rahmen dieses Ablaufs bestehen einige Möglichkeiten den Datenverkehr zwischen den beteiligten Systemen umzuleiten und sich als Angreifer logisch zwischen der Workstation und dem jeweils anderen System zu positionieren. Derartige Angriffe werden, wie in der Einleitung bereits ausgeführt als als Man-in-the-middle Attacks (MITM) bezeichnet.

3. DHCP-Spoofing

DHCP-Spoofing macht sich die Tatsache zu Nutze, dass zum Auffinden von DHCP-Servern ein Broadcast eingesetzt wird. Gelingt es dem Angreifer vor dem autorisierten DHCP-Server eine Antwort an die Workstation zu übermitteln, so kann er sowohl die IP-Adresse des Default Routers, als auch die der zu verwendenden DNS-Server nach belieben manipulieren.[7] So kann er sein eigenes System als Default Router eintragen, wodurch alle von der Workstation in andere Netzwerke versendeten Datenpakete zunächst über sein System geleitet werden, bevor sie an den autorisierten Default Router gelangen.

4. ARP-Spoofing

Da der ARP-Request zur Auflösung einer IP-Adresse aus dem lokalen Netzwerk in die entsprechende MAC-Adresse als Broadcast versendet wird, kann ein Angreifer, dem es gelingt vor dem eigentlich angesprochenen Server mit einer falschen MAC-Adresse[8] zu antworten, den gesamten vom Opfer an den Server gerichteten Datenverkehr über ein System seiner Wahl umleiten.[9] Primärziel der Angreifer ist es meist, die MAC-Adresse des Default Routers oder eines lokalen DNS-Servers zu „spoofen".

5. DNS-Spoofing

Zur Auflösung eines Domainnamens in eine IP-Adresse wird ein DNS-Request vom Client an den eingetragenen DNS-Server übermittelt. Um die Antworten des DNS-Servers konkreten Anfragen zuordnen zu können, enthält jeder DNS-Request eine ID, die im zugehörigen Response enthalten sein muss. Gelingt es einem Angreifer von der ID eines versendeten Requests Kenntnis zu erlangen, so kann er versuchen, einen gefälschten Response vor dem DNS-Server an den Client zu übermitteln.[10]

6. DNS-Poisoning

Als DNS-Caching[11] wird die zeitlich begrenzte Zwischenspeicherung von einmal abgefragten Informationen anderer Name-Server bezeichnet. Jeder Name-Server betreibt Caching um eine höhere Leistungsfähigkeit zu erreichen und die Anfragelast im weltweiten Domain Name System zu reduzieren. Unter Cache Poisoning versteht man die nicht autorisierte Einflussnahme auf die zwischengespeicherten DNS-Daten anderer Server.[12] Meist erfolgt dies

[7] Die später einlangende Antwort des autorisierten DHCP-Servers wird verworfen.
[8] Zur ähnlichen Funktionsweise von Proxy ARP, siehe *Stevens*, 60 ff.
[9] Die später einlangende Antwort des autorisierten Systems wird verworfen.
[10] Die später einlangende Antwort des autorisierten DNS-Servers wird verworfen.
[11] *Albitz/Liu*, S. 34 ff
[12] Dies erfordert das Vorliegen einer Sicherheitslücke wie CVE-2005-0817 oder CVE-2005-0877; vgl ausführlich *Feiler*, Zur strafrechtlichen Beurteilung von IT-Sicherheitslücken, 49

durch das unaufgeforderte Senden gefälschter DNS-Responses. Obgleich die so erhaltenen Daten vom Name-Server niemals angefordert wurden, werden sie oft dennoch in den Cache aufgenommen. Dies führt dazu, dass es einem Angreifer möglich ist, den Cache derart zu manipulieren, dass alle Anfragen nach der Auflösung eines bestimmten Domainnamens (zB www.amazon.com) mit eine IP-Adresse seiner Wahl beantwortet werden.[13]

7. Strafrechtliche Beurteilung von Man-in-the-Middle Attacks

Im Folgenden werden die unterschiedlichen Formen von Man-in-the-Middle Attacks in Bezug auf eine Strafbarkeit nach österreichischem Recht untersucht.

7.1. Man-in-the-Middle Attack zwecks Denial of Service

Der Angreifer kann als „Man-in-the-Middle" die Kommunikation jederzeit unterbrechen. Ebenso kann er bei einem DHCP-Spoofing eine nicht vergebene oder gar keine IP-Adresse als Default Router oder als DNS-Server angeben oder bei DNS-Spoofing bzw DNS-Poisoning einen Domainnamen in eine nicht existente IP-Adresse auflösen. All diese Vorgehensweisen führen dazu, dass in gewissem Umfang ein Denial of Service (DoS) eintritt. Nach § 126b StGB ist jedoch nur die „schwere" Störung der Funktionsfähigkeit eines Computersystems iSd § 74 Abs 1 Z 8 strafbar.[14] Als Objekt der Störung kommen das Client-System, das Server-System und das lokale Netzwerk in Betracht. Wird beispielsweise durch ein kontinuierliches DNS-Spoofing die Anfrage eines Clients nach der IP-Adresse von www.amazon.com mit einer nicht existenten IP-Adresse beantwortet, sodass dieses Client-System für einen gesamten Tag keine Verbindung zu www.amazon.com herstellen kann, so ist wohl weder das Client-System noch das lokale Netzwerk schwer gestört, da mit amazon.com kommunizieren zu können, nur einen geringen Teil der bereitgestellten Funktionalität darstellt. Auch das Server-System amazon.com ist durch den Verlust eines von Zig-Millionen potentiellen Clients nicht als schwer gestört anzusehen. Wird hingegen durch DHCP- oder ARP-Spoofing die Internetkommunikation gänzlich unterbunden, so liegt jedenfalls eine schwere Störung des lokalen Netzwerkes vor.

7.2. Man-in-the-Middle Attack zwecks Sniffing

Da bei allen Formen von Man-in-the-Middle Attacks der Datenverkehr über ein System des Angreifers umgeleitet wird, ist es für ihn grundsätzlich ein Leichtes sich von diesen Daten Kenntnis zu verschaffen.[15] Für eine Strafbarkeit kommen insbesondere die §§ 119 und 119a in Betracht. Der objektive Tatbestand beider Delikte erfordert das Verwenden einer Abhörvorrichtung, was hier problemlos gegeben sein wird. Handelt der Täter mit der Absicht sich von einer Nachricht (dh Inhaltsdaten) Kenntnis zu verschaffen, so kommt eine Strafbarkeit nach § 119 StGB in Betracht. Bezieht sich die Spionageabsicht hingegen nur auf Daten, die keine Gedankenerklärung darstellen[16], so tritt gem § 119a StGB erst dann eine Strafbarkeit ein, wenn zur Spionageabsicht eine Verwendungsabsicht und eine Gewinn- bzw. Schädigungsabsicht hinzutritt.

Speichert der Angreifer „gesniffte" Nachrichten, so kommt – subsidiär zu § 119 StGB – eine Strafbarkeit nach § 120 Abs 2a StGB in Betracht.

---

[13] Zu der negativ zu beantwortenden Frage nach einer Strafbarkeit nach §§ 118a oder § 126a vgl *Feiler*, Zur strafrechtlichen Beurteilung von IT-Sicherheitslücken, 49

[14] Zur erforderlichen Schwere der Störung vgl *Feiler*, Zur strafrechtlichen Beurteilung von IT-Sicherheitslücken, 22 ff

[15] Dies trifft insbesondere bei der Verwendung von unverschlüsselten Protokollen wie FTP, POP3, IMAP oder HTTP zu.

[16] zB ein automatisch generiertes E-Mail, das Kennzahlen bezüglich der Sicherheit eines Systems enthält.

Verschafft sich der Angreifer durch das Sniffing Kenntnis von Authentifizierungsdaten mit dem Vorsatz eines der Computerdelikte (§§ 118a, 119, 119a, 126a, 126b, 148a) zu begehen, so tritt eine Strafbarkeit nach § 126c Abs 1 Z 2 ein.[17]

7.3. Man-in-the-Middle Attack zwecks Phishing

Durch einen Man-in-the-Middle Attack können HTTP-Requests, die beispielsweise an eine Website einer Bank gerichtet sind, leicht auf eine täuschend ähnlich aussehende Website umgeleitet werden, die zur Eingabe von Authentifizierungsdaten (und im Falle einer Bank TANs) auffordert.

Für eine strafrechtliche Beurteilung ist es zweckmäßig den Sachverhalt in zwei Abschnitte zu unterteilen.[18]

1. Die Phishing-Phase: im Rahmen dieses Sachverhaltsabschnittes führt der Angreifer den Man-in-the-Middle Attack aus.

2. Die Verwertungs-Phase: die in Phase 1 erlangten Daten werden verwendet um das Konto des getäuschten Benutzers zu belasten und sich oder einem anderen einen Vermögensvorteil zu verschaffen.

7.3.1. Die Phishing-Phase

Zunächst kommt eine Strafbarkeit nach § 146 StGB in Betracht. Der Tatbestand des Betruges erfordert, dass der Getäuschte sich oder einen anderen durch eine Handlung, Duldung oder Unterlassung am Vermögen schädigt. Die bei Phishing vom Getäuschten vorgenommene Handlung der Preisgabe bestimmter Daten stellt jedoch noch keinen Vermögensschaden dar. Ein solcher tritt erst durch die Handlungen eines Dritten, der die Daten zur Belastung des Kontos verwendet, ein. Mangels Selbstschädigung bzw mangels Unmittelbarkeit des Schadenseintritts ist eine Strafbarkeit nach § 146 StGB für die Phishing-Phase zu verneinen.

Eine Versuchsstrafbarkeit nach § 146 iVm § 15 StGB scheitert schon daran, dass dem Täter bewusst sein wird, dass es zur Vermögensschädigung noch weiterer Handlungen (nämlich der Belastung des Kontos) bedarf. Insofern ist die aktionsmäßige Nähe zur Tatausführung nicht gegeben.

Ein weiterer in Betracht kommender Straftatbestand ist § 108 StGB. Nach dem Wortlaut des § 108 ist strafbar, wer einen anderen „in seinen Rechten“ dadurch schädigt, dass er ihn oder einen Dritten durch Täuschung über Tatsachen zu einer Handlung, Duldung oder Unterlassung verleitet, die den Schaden herbeiführt. Legt man (wie fallweise die Judikatur) dem durch § 108 geschützten Rechtsgut ein weites Verständnis zugrunde, so wäre es durchaus denkbar, auch das Grundrecht auf Datenschutz (§ 1 DSG 2000) unter den Begriff der Rechte des § 108 zu subsumieren. Handelt es sich bei den von dem Getäuschten übermittelten Daten um personenbezogene Daten des Getäuschten, so könnte hierdurch das Grundrecht auf Datenschutz des Getäuschten verletzt sein (vgl § 7 Abs 2 DSG 2000). In aller Regel wird es sich um indirekt personenbezogene Daten (vgl § 4 Z 1 DSG 2000) handeln, da die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmbar ist. (zB 2009898098/9jllweycv als Benutzername/Passwort). Eine Strafbarkeit nach § 108 könnte bei einem weiten Verständnis der Norm daher für die Phishing-Phase bejaht werden.[19] Dem ist entgegenzuhalten, dass bei einer derart ausdehnenden Auslegung der rechtsstaatlich äußerst

[17] vgl *Feiler*, Zur strafrechtlichen Beurteilung von IT-Sicherheitslücken, 7 ff
[18] *Bergauer*, RZ 2006, 82
[19] so *Bergauer*, RZ 2006, 82

bedeutende Grundsatz „keine Strafe ohne Gesetz“ (§ 1 StGB) weitestgehend unterlaufen würde. Die hL sieht für § 108 StGB daher keinen Anwendungsbereich. ME ist der strafrechtliche Schutz des Grundrechts auf Datenschutz als durch § 51 DSG 2000 abschließend geregelt anzusehen und eine Strafbarkeit nach § 108 strengstens abzulehnen.[20]

Die Datenfälschung gem § 225a StGB ist dem Delikt der Urkundenfälschung (§ 223 StGB) nachempfunden. In der Phishing-Phase werden durch die Erstellung der Phishing-Site vom Täter falsche Daten hergestellt, die den Anschein erwecken, dass die Website von einer anderen Person betrieben würde. Dies erfüllt den objektiven Tatbestand des § 225a. Neben dem Tatbildvorsatz ist idR auch der erweiterte Vorsatz, die falschen Daten im Rechtsverkehr zum Beweis eines Rechtsverhältnisses zu gebrauchen, gegeben. Denn der Täter will unzweifelhaft über das Bestehen eines Rechtsverhältnisses mit dem Betreiber der Phishing-Site täuschen. Eine Strafbarkeit nach § 225a StGB ist daher idR zu bejahen.

Da in den hier behandelten Fällen das Phishing nicht durch das Versenden von E-Mails, sondern durch einen Man-in-the-Middle Attack erfolgt, ist weiters eine Strafbarkeit nach §§ 119, 119a denkbar. Insbesondere ist näher zu prüfen ob der Täter eine Vorrichtung iSd §§ 119, 119a benützt und ob es sich um Daten handelt, die „nicht für ihn bestimmt“ sind. Art 3 CyCC spricht von „technical means“ durch die das Abfangen der Daten zu erfolgen hat. Der erläuternden Bericht zur CyCC vom 8.11.2001 Rz 53 führt hierzu erhellend aus: „The requirement of using technical means is a restrictive qualification to avoid over-criminalisation.” Entscheidend ist mE hierbei, dass bei E-Mail Phishing das Opfer durch eine Täuschung dh ohne den Einsatz von „technical means“ zur Preisgabe der Daten bewegt wird und die Kommunikationsverbindung zwischen Opfer und Phishing-Site ohne technische Eingriffe des Täters gänzlich standardkonform abgewickelt wird. Bei einem Phishing durch einen Man-in-the-middle Attack wird hingegen die Kommunikationsverbindung – sei es durch DNS-Poisoning, DHCP-, ARP- oder DNS-Spoofing – vom Angreifer auf nicht standardkonforme Weise manipuliert, wodurch das Abfangen der Daten nicht nur durch eine Täuschung sonder maßgeblich durch den Einsatz von „technical means“ erfolgt. Daher stellt ein Man-in-the-middle Attack im Zusammenhang mit einer Phishing-Site mE eine Vorrichtung iSd § 119, 119a dar. Weiters ist zu prüfen, ob es sich bei den Daten um nicht für den Angreifer bestimmte Daten handelt. Da sowohl nach subjektiven Kriterien, dh nach der Vorstellung des Opfers als auch nach objektiven Kriterien, dh bei standardkonformer Abwicklung der Kommunikationsverbindung die Daten nicht an den Angreifer sondern einen Dritten übertragen worden wären, ist auch dieses Tatbestandsmerkmal als erfüllt anzusehen. Damit ist – ein entsprechender Vorsatz vorausgesetzt – eine Strafbarkeit nach §§ 119, 119a grundsätzlich zu bejahen.

Abschließen kommt eine Strafbarkeit nach § 126c Abs 1 Z 2 in Betracht. Nach § 126c Abs 1 Z 2 ist strafbar, wer ein Passwort mit dem Vorsatz, dass es zur Begehung eines Computerdelikts (§§ 118a, 119, 119a, 126a, 126b, *148a*) gebraucht wird, herstellt, einführt, vertreibt, veräußert, sonst zugänglich macht, sich verschafft oder besitzt. Das in der Phishing-Phase erfolgende Sichverschaffen bzw das nachfolgende Besitzen erfüllt daher den objektiven Tatbestand. Die Strafbarkeit hängt va vom subjektiven Tatbestand ab. Denn nur wenn man für die Verwertungsphase eine Strafbarkeit nach § 148a StGB bejaht, ist ein für § 126c Abs 1 Z 2 relevanter Vorsatz gegeben. Beurteilt man hingegen die Verwertungsphase nur nach § 146, so hat der Täter in der Phishing-Phase nur einen Vorsatz § 146 jedoch nicht § 148a zu begehen.

[20] mwN *Feiler*, Social Engineering

Für die Phishing-Phase kann daher zusammenfassend gesagt werden, dass idR eine Strafbarkeit nach § 225a, § 119 oder § 119a und abhängig von der rechtlichen Beurteilung der Verwertungs-Phase nach § 126c Abs 1 Z 2 eintritt.

7.3.2. Verwertungs-Phase

Für die Verwertungs-Phase kommt nur eine Strafbarkeit nach § 146 StGB (Betrug) und § 148a StGB (betrügerischer Datenverarbeitungsmissbrauch) in Betracht. Grundsätzlich erfordert § 146 die Täuschung eines Menschen, § 148 hingegen die „Täuschung" einer Maschine. ME kommt eine Strafbarkeit nach § 146 daher nur in Betracht, wenn der Täter die in der Phishing-Phase erlangten Daten gegenüber einer natürlichen Person einsetzt (zB Phonebanking). In allen anderen Fällen müsste mE eine Subsumtion unter § 148a erfolgen. Ohne diesen Meinungsstreit hier näher untersuchen zu können, sei darauf hingewiesen, dass diese Frage für eine Strafbarkeit nach § 126c Abs 1 Z 2 StGB (im Rahmen der Phishing-Phase) von erheblicher Bedeutung ist.

7.4. Man-in-the-Middle Attack zwecks Hacking

Man-in-the-Middle Attacks können auch dazu dienen, sich Zugang zu einem Computersystem zu verschaffen. Hierfür kommt va eine Strafbarkeit § 118a StGB in Betracht.

7.4.1. Hacking des Clients durch Code Injection

Da der gesamte Datenverkehr über ein System des Angreifers umgeleitet wird, ist es für diesen idR ein Leichtes, Daten in den Datenstrom einzuschleusen.[21] Sendet das Opfer beispielsweise einen HTTP-Request für eine Datei mit der Endung .exe (dh eine ausführbare Anwendung), so könnte der Angreifer im HTTP-Response Malware[22] an das Opfer senden. Ebenso könnte der Angreifer bösartigen Script-Code in einen HTTP-Resonse integrieren, der dann in der Sicherheitszone der Website zur Ausführung gelangt.

Bei derartigem Vorgehen stellt sich in Bezug auf § 118a StGB vornehmlich die Frage, ob sich der Angreifer durch die Verletzung einer Sicherheitsvorkehrung im Computersystem Zugang verschafft. Eine Verletzung ist mE keinesfalls in der regulären Ausführung des Codes auf dem System des Opfers zu erblicken. Allenfalls könnte es zu einem früheren Zeitpunkt des Man-in-the-middle Attacks zu einer solchen Verletzung gekommen sein.

Bei DHCP-, ARP- und DNS-Spoofing handelt es sich tatsächlich um die Ausnützung einer sog Race Condition[23] (gleichsam ein „Wettlauf" zweier Prozesse). Da es hierbei zu keiner Verletzung der Integrität von Daten kommt, ist eine Strafbarkeit nach § 118a StGB für durch DHCP-, ARP- oder DNS-Spoofing erfolgtes Hacking zu verneinen.

Bei einem DNS-Poisoning sendet der Angreifer unaufgeforderte DNS-Responses an den DNS-Server, die dieser aufgrund einer Sicherheitslücke in seinem Cache speichert. Zu einer Verletzung der Datenintegrität kommt es aber nur in jenen Fällen, in denen der DNS-Server einen bestehenden Eintrag mit dem neu erhaltenen ersetzt. Sofern die ausgenützte Sicherheitslücke darin besteht DNS-Responses vor der Speicherung im Cache schlicht nicht zu überprüfen, so ist mE bereits das Vorliegen einer Sicherheitslücke zu verneinen. Ist jedoch beispielsweise wie bei CVE-2005-0877[24] die DNS Query-ID durch einen Brute Force Attack

[21] Dies kann durch den Einsatz asymmetrischer kryptographischer Verfahren und einer Public Key Infrastructure (PKI) wesentlich erschwert werden.
[22] Ein Überbegriff für Viren, Würmer, trojanische Pferde, Adware, Spyware (inklusive KeyLogger) und sonstige Schadsoftware.
[23] ausführlich *Feiler*, Zur strafrechtlichen Beurteilung von IT-Sicherheitslücken, 35 f
[24] vgl http://nvd.nist.gov/nvd.cfm?cvename=CVE-2005-0877 und http://xforce.iss.net/xforce/xfdb/19826

ermittelbar, ist mE die Verletzung einer Sicherheitsvorkehrung durch die Verwendung von Authentifizierungsdaten[25] gegeben. Denn ähnlich einer Session-ID[26] dient eine Query-ID dazu, den DNS-Server an den ein Request gerichtet wurde, einmalig zu identifizieren. Es stellt sich hier jedoch das auch bei Cross Site Scripting (XSS)[27] auftretende Problem, dass sich der Angreifer Zugang zu einem Computersystem verschafft indem er eine Sicherheitsvorkehrung in einem anderen verletzt. Da beide Computersysteme jedoch Teil eines Netzwerkes (des Internets) sind, ist dieses als Tatobjekt zu behandeln. Da sich der Täter Zugang zu einem Teil des Netzwerkes verschafft (dem Client-System) indem er eine, im Netzwerk befindliche Sicherheitsvorkehrung verletzt, besteht für diesen Sonderfall der Code Injection durch DNS-Poisoning – unter den sonstigen Voraussetzungen – eine Strafbarkeit nach § 118a StGB.

7.4.2. Hacking des Servers durch Code Injection

Da der Angreifer auch die vom Client an den Server gesendeten Daten manipulieren kann[28], gilt grundsätzlich zu 7.4.1. Gesagtes.

7.4.3. Hacking des Servers durch Verwendung gesniffter Authentifizierungsdaten

Das Sniffing von Authentifizierungsdaten ist bereits nach § 126c Abs 1 Z 2 StGB strafbar (s.o.). § 126c Abs 1 Z 2 stellt das Sichverschaffen von Authentifizierungsdaten unter Strafe, wenn es mit dem Vorsatz erfolgt, § 118a zu begehen. Somit ist die Vorbereitung eines Hackings unter Verwendung von Authentifizierungsdaten grundsätzlich strafbar. Hieraus ergibt sich, dass das Tatbestandsmerkmal der „Verletzung" einer Sicherheitsvorkehrung in § 118a StGB – im Rahmen des äußerst möglichen Wortsinns – entsprechend systematisch zu interpretieren ist. Daher erfüllt die Zugangsverschaffung unter Verwendung gesniffter Authentifizierungsdaten den objektiven Tatbestand des § 118a.[29] Ist neben dem Tatbildvorsatz kumulativ auch eine Spionage-, Verwendungs- und Gewinn- bzw. Schädigungsabsicht gegeben, so besteht eine Strafbarkeit nach § 118a StGB.

8. Quellen

Albitz/Liu, DNS and BIND[4], O'Reilly, Sebastopol 2001

Bergauer, Phishing im Internet – eine kernstrafrechtliche Betrachtung, RZ 2006, 82

Cooper/Northcutt/Fearnow/Frederick, Intrusion Signatures and Analysis, Sams, Indiana 2001

Cox/Gerg, Managing Security with Snort and IDS Tools, O'Reilly, Sebastopol 2004

Feiler, Zur strafrechtlichen Beurteilung von IT-Sicherheitslücken, 2006, http://www.lukasfeiler.com/Zur_strafrechtlichen_Beurteilung_von_IT-Sicherheitsluecken.pdf

Feiler, Threat Update: Social Engineering, 2006, http://www.e-center.eu/ecenter/threatupdate/Social_Engineering.pdf

Hamm, Appliance gegen ARP-basierte Angriffe, iX 1/2006, S. 92

[25] Zu einer systematischen Interpretation von § 118a und § 126c Abs 1 Z 2 siehe unter 7.4.3.
[26] vgl *Feiler*, Zur strafrechtlichen Beurteilung von IT-Sicherheitslücken, 32 f
[27] vgl *Feiler*, Zur strafrechtlichen Beurteilung von IT-Sicherheitslücken, 32 f
[28] Besonders effektiv beispielsweise durch das Einschleusen von Befehlen in eine Telnet- oder SSH1-Session.
[29] vgl *Feiler*, Zur strafrechtlichen Beurteilung von IT-Sicherheitslücken, 16

Hamm, Gefahrenabwehr im Intranet, iX 10/2006, S. 50

Kirch/Dawson, The Linux Network Administrator's Guide², O'Reilly, Sebastopol 2000; als Open Book online verfügbar unter http://www.tldp.org/guides.html

Northcutt/Novak, Network Intrusion Detection, Sams, Indiana 2003

Northcutt/Zeltser/Winters/Fredrick/Ritchey, Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPNs), Routers, and Intrusion Detection Systems, Sams, Indiana 2002

McNab, Network Security Assessment, O'Reilly, Sebastopol 2004

Peikari/Chuvakin, Security Warrior, O'Reilly, Sebastopol 2004

Stevens, TCP/IP Illustrated, Volume 1, Addison-Wesley, Boston 1994

Wegener/Dolle, Spoofing: gefälschte Adressen und gekaperte Server, iX 3/2005, S. 110