

# Externe Innentäter

## Eingeschleuste Hardware erhöht Gefährdung durch ARP-Angriffe

**Nicht jeder Angriff von innen muss von einem klassischen Innentäter erfolgen. Auch Externe können sich leicht „internen“ Zugriff auf Netzwerke verschaffen. Umso wichtiger sind Maßnahmen gegen Attacken auf den Datenfluss im LAN.**

*Von Andreas Rieke, Hagen*

Im Dezember 2003 wurde in Haifa (Israel) ein Einbruch in eine Filiale der Post gemeldet; die Sicherheitskräfte waren kurze Zeit später vor Ort, konnten jedoch keinen Täter mehr entdecken. Eine kurze Durchsuchung der Räumlichkeiten ergab, dass nichts fehlte, also wurden die Scheiben wieder eingesetzt und der Vorfall vergessen. Wenige Wochen später fiel durch statistische Überprüfungen auf, dass immer wieder Gelder auf neu eröffnete Konten übertragen und dann relativ schnell abgehoben wurden. Alle diese auffälligen Transaktionen initiierte genau die Filiale, die überfallen worden war. Bei einer daraufhin veranlassten erneuten Durchsuchung fand man ein kleines Wireless Device, das nicht zur Ausstattung der Post gehörte (<http://catless.ncl.ac.uk/Risks/23.13.html#subj3>).

Details des Vorgangs sind zwar nicht veröffentlicht worden, doch mit etwas Vorstellungskraft kann man den folgenden, denkbaren Tathergang mutmaßen: Möglicherweise operierten die Täter aus einem Fahrzeug, das vor der Postfiliale abgestellt war, und konnten so per WLAN ohne bemerkenswertes Risiko Zugriff auf das interne Netz der Post nehmen. Zum Zugriff auf die Transaktionsabwicklung könnten sie entweder über Insiderwissen verfügt oder die notwendigen Informationen durch Hacking im internen Netz beschafft haben.

Beispielsweise ermöglichen es Attacken auf das Address Resolution Protocol (ARP, s. u.) einem Angreifer in aller Regel – selbst in einem vollständig gewitchten Netz – als Man-in-the-Middle in jegliche Kommunikation einzudringen, Daten abzuhören, Passworte zu sammeln und Daten zu manipulieren; bei ungenügender Prüfung von Zertifikaten lassen sich so selbst verschlüsselte Verbindungen (SSL, SSH oder PPTP) angreifen. Auf diese Art wäre es für die Täter leicht gewesen, auch in vormals legitime Transaktionen beispielsweise die eigene Kontonummer als Empfänger einzusetzen.

Der Vorfall in Israel ist der erste dem Autor bekannte „Überfall“ dieser Art, aber wohl kaum der letzte. WLAN-Devices oder Ähnliches in fremde Netze einzuschleusen, erscheint recht einfach – längst nicht immer ist dazu ein Einbruch notwendig. Und neben unmittelbaren finanziellen Auswirkungen sind auch Spionage- und Imageschäden leicht vorstellbar. Insofern richtet sich diese Art der Bedrohung nicht nur gegen Banken und Finanzdienstleister, sondern gegen jeden, der sensitive Daten verarbeitet – vom Großkonzern mit milliardenschweren Geschäftsgeheimnissen bis hin zum Anwalt oder Arzt, der heikle Informationen vorhält.

Ein großer Vorteil für Angreifer ist dabei, dass die Bedrohung

durch interne Angriffe auf den unteren Protokollschichten oft unterschätzt wird (vgl. auch [2]). Oft begegnet man der Argumentation, dass hierzu ja Mitarbeiter das eigene Unternehmen attackieren müssten, was man – trotz gegenteiliger Aussagen durch Studien – gerne als abwegig ansieht. Spätestens mit der Verbreitung kleiner und leistungsfähiger drahtloser Netzwerkhardware ist jedoch die Grenze zwischen Innen- und Außentäter erheblich unschärfer geworden.

### ARP-Angriffe

Wer einmal einen „Fuß in der Tür“ hat, kann natürlich alle üblichen Hacking-Register ziehen. Selbst bei wirksamer Absicherung aller Dienste und Applikationen, bleiben dabei meist die „tieferliegenden“ Kommunikationskanäle angreifbar, beispielsweise über ARP-Angriffe, allem voran das so genannte ARP-Poisoning. Das Address Resolution Protocol (ARP, RFC 826) dient Netzwerkhardware dazu, dynamisch die Ethernet-Adresse (MAC-Adresse) eines Systems zu ermitteln, von dem bis dato nur die IP-Adresse bekannt ist. ARP Poisoning bezeichnet die gezielte Manipulation der Zwischenspeicher (Caches) zweier an einer Kommunikationsbeziehung beteiligter Maschinen, um ihre gesamte Kommunikation über das System eines Angreifers umzuleiten (Man-in-the-Middle). Dazu muss dieser lediglich (mindestens) einmal pro Minute zwei ARP-Pakete verschicken.

Im Prinzip könnte man versuchen, auf ARP gänzlich zu verzichten und stattdessen nur statische Einträge zu verwenden. Dies ist jedoch aufgrund des hohen Konfigurationsaufwands und mangelnder Fehlertoleranz (keine Kommunikation nach Austausch einer defekten Netzwerkkarte) in größeren Netzen praktisch unmöglich.

Auch der Versuch, das Ausführen fremder Software innerhalb

der Unternehmens-Infrastruktur zu verhindern, scheitert spätestens dann, wenn – wie im geschilderten Beispiel – fremde Hardware im eigenen Netz platziert wird. Ende-zu-Ende-Verschlüsselung, Authentifizierung von Daten und Kommunikationspartnern sowie Integritätsprüfungen könnten sicherlich helfen, bedeuten allerdings erheblichen Aufwand und werden in der Praxis noch viel zu wenig eingesetzt.

## Abwehrprobleme

Intrusion Detection Systems sind ebenfalls unwirksam: Zum einen müsste man sie unternehmensweit (in jedem Subnetz) einsetzen und selbst dann könnte man ARP-Angriffe nur dann erkennen, wenn Zuordnungen zwischen IP- und MAC-Adresse klar definiert sind, was aus Kosten- und Flexibilitätsgründen kaum möglich erscheint (dann wäre z. B. keine dynamische Vergabe von IP-Adressen per DHCP mehr möglich). An dynamischen IP-Adressen scheitert auch arpwatch (<http://www.nrg.ee.lbl.gov/>), ein am Lawrence Berkeley National Laboratory (LBNL) entwickeltes Tool zum Schutz vor ARP-Angriffen.

Der Vollständigkeit halber sei erwähnt: Da ARP-Angriffe nur innerhalb eines Subnetzes möglich sind, liegt eine weitere Alternative darin, möglichst kleine Subnetze zu bilden – theoretisch idealerweise mit nur einem PC und dem Router; die Hersteller wären über entsprechende Aufträge sicherlich erfreut...

Unter Unix sind zwar Schutzfunktionen im IP-Stack verfügbar, diese können jedoch – besonders im Zusammenspiel mit Cluster-, Hochverfügbarkeits- oder Load-Balancing-Lösungen – zu Fehlfunktionen führen. Und die Einschränkung von Verkehrsbeziehungen, beispielsweise durch Virtual LANs (VLANs) oder Cisco Port Protection, erscheint zum einen recht aufwändig und kann zudem deutlich eingeschränkte Funktionalität zur Folge haben.

## Literatur

- [1] Andreas Rieke, Vertraulichkeit ade wegen ARP-Spoofing-Angriffen, ntz, Heft 2-3, März 2004
- [2] Felix Lindner, Auf Sand gebaut, Angreifbarkeit von aktiven Netzwerkkomponenten, 2003#4, S. 6
- [3] Jürgen Schmidt, Spionage am Arbeitsplatz: So kommen neugierige Kollegen an Ihre Daten, c't 12/2001, S. 232
- [4] Thomas Demuth, Interner Zugriff, Angriffstechnik im lokalen Netz: ARP-Spoofing und -Poisoning, Linux Magazin 06/2004, S. 34

Wenn sich ARP-Angriffe auch nicht ohne übermäßigen Aufwand oder große Einschränkungen gänzlich ausschließen lassen, so bleibt doch die Möglichkeit, ein System zu implementieren, dass Angriffsversuche erkennen kann und eingreift, bevor diese Wirkung zeigen. Dazu müsste man zunächst manipulierte ARP-Pakete oder ARP-Caches aufspüren. Handhabbaren Schutz vor ARP-Angriffen versprechen somit Lösungen, die einerseits Zugriff auf lokale (Sub-)Netze und ARP-Caches haben und andererseits über ein zentrales Management-System verfügen; hierzu existieren im Markt zwei kommerzielle Ansätze (siehe Kasten).

## Fazit

Interne Angriffe bieten aufgrund des direkten Zugriffs auf das LAN ein weitaus höheres Bedrohungspotenzial als Attacken von außen. Insofern sollten heutzutage bei Vorliegen sensibler Daten und Kommunikationswege Schutzmaßnahmen im „Netzhinterland“ den Perimeter-schutz ergänzen. Entsprechende Sicherungen zu ergreifen, bedeutet nicht, vor allem die eigenen Mitarbeiter

unter Generalverdacht zu stellen. Nur allzu leicht erhalten schließlich auch Besucher, externe Dienstleister, Eindringlinge oder sonstige Personen entgegen der Security-Policy Zugriff auf das interne Netz. Gleichzeitig helfen die Maßnahmen natürlich auch gegen „schwarze Schafe“ in den eigenen Reihen, wie Praktikanten oder Mitarbeiter, die innerlich bereits gekündigt haben und gegen das Unternehmen arbeiten oder sich als Industriespion verdingen. Schutz vor all solchen Tätern ist heutzutage kaum

realisiert, und wenn Angriffe überhaupt festgestellt werden, ist es meist schon zu spät. Dass beim „Bankraub“ in Israel tatsächlich Verdächtige festgenommen wurden, darf auch nicht darüber hinwegtäuschen, dass dies im Normalfall kaum möglich sein wird. ■

*Dr. Andreas Rieke (andreas.rieke@isl.de) ist Geschäftsführer der ISL Internet Sicherheitslösungen GmbH.*

## Kommerzielle Lösungen gegen ARP-Angriffe

**Selbst wo das Thema ARP-Angriffe und ihr Gefahrenpotenzial den Verantwortlichen bekannt ist, wird in der Regel keine Abhilfe geschaffen. Der Grund ist dabei weniger Blauäugigkeit als das „dünne“ Angebot professioneller Lösungen. Lediglich Cisco und ISL liefern entsprechende Systeme, die auch den Anforderungen großer Installationen genügen.**

### Dynamic ARP Inspection

In den Switches der Catalyst-Produktreihe hat Cisco ([www.cisco.com/global/DE/](http://www.cisco.com/global/DE/)) mit den so genannten Smartports die Dynamic ARP Inspection (DAI) eingeführt. Dabei wird jedes ARP-Paket (Requests und Replies) gegen eine Switch-interne Datenbank von MAC-IP-Adresspaaren gegengeprüft. Sind die in einem Paket enthaltenen Adressen nicht plausibel, wird es verworfen, andernfalls die interne Datenbank aktualisiert und das ARP-Paket an den entsprechenden Port weitergeleitet. Entscheidend für das Vereiteln eines ARP-Angriffes ist die Korrektheit der Zuordnungen in der Datenbank, die durch das Beobachten und Auswerten von DHCP-Paketen erzeugt und aktualisiert wird. Als weitere Möglichkeit bietet sich das manuelle Eintragen als korrekt geltender MAC-IP-Paare durch den Netzadministrator an. Weiterhin verwirft der Switch ARP-Pakete, die IP-Adressen enthalten, die nicht in der Datenbank vertreten sind, oder wenn die MAC-Adresse in dem ARP-Paket nicht mit derjenigen im Ethernet-Header übereinstimmt. DAI wird allerdings auf als vertraut (trusted) deklarierten Ports nicht angewendet. Wer von der Vergabe des trusted-Attributs zu großzügig Gebrauch macht, geht daher die Gefahr von Sicherheitslöchern ein. Mit untrusted-Ports ist jedoch (als Standardwert) eine Degradierung der Übertragungsrates auf 15 ARP-Pakete pro Sekunde verbunden. Falls mehr ARP-Pakete den Port erreichen, wird dieser abgeschaltet (errdisable state) und muss im ungünstigsten Falle vom Administrator explizit wieder freigeschaltet werden.

### ARP-Guard

Das System ARP-Guard der Firma ISL Internet Sicherheitslösungen GmbH ([www.arp-guard.com](http://www.arp-guard.com)) analy-

siert die ARP-Pakete innerhalb eines Netzsegments und führt eine interne Datenbank über MAC-IP-Adresspaare. Operative Elemente sind Sensoren, die über eine Management-Konsole mit Web-Interface konfiguriert und überwacht werden. ARP-Guard-Sensoren sind als Software für Linux (SuSE und Red Hat) und Microsoft Windows verfügbar; die Management-Konsole läuft auf Linux. In Kooperation mit der Celestix Networks GmbH ist ARP-Guard auch als Appliance erhältlich. Die so genannten LAN-Sensoren von ARP-Guard arbeiten direkt an den Spiegel-Ports der zu überwachenden (programmierbaren) Switches, wodurch das System sämtliche Pakete, die den Switch passieren, kontrollieren kann. Bei größeren Netzen ist eine Kaskadierung solcher LAN-Sensoren möglich. Alternativ gibt es SNMP-Sensoren, die alle notwendigen Informationen von den Routern per Simple Network Management Protocol (SNMP, RFC 1157) abrufen.

Für die Interpretation der Sensoren-Meldungen ist das Management-System verantwortlich, das über verschlüsselte Verbindungen mit den Sensoren kommuniziert. Dort werden auch erkannte Angriffe dargestellt; bei entsprechender Pflege des Systems bis hin zur Benennung des Arbeitsplatzrechners, von dem aus ein Angriff erfolgt. Eine Alarmierung des Verantwortlichen kann über E-Mail oder SMS erfolgen. ARP-Guard ist in der Lage, berechnete Änderungen an MAC-IP-Adresspaaren von Angriffen zu unterscheiden (z. B. bei Neuvergabe einer IP-Adresse per DHCP) und kann daher auch als Werkzeug dienen, um IP-Adresskonflikte oder fehlerhaft arbeitende DHCP-Server aufzuspüren. Bei erkannten Angriffen kann ARP-Guard automatisch Gegenmaßnahmen einleiten und den (Switch-)Port, an dem der Angreifer sitzt, herunterfahren. Sollte dies nicht möglich sein, da der korrespondierende Switch nicht programmierbar ist, ermittelt das System den nächsten programmierbaren Switch und deaktiviert dort den entsprechenden Port.

*Dr. Thomas Demuth (thomas.demuth@thomas-demuth.de) ist IT Security-Berater.*