Netzwerkschutz auf Layer 2

Schutz gegen ARP-Attacken

LANs sind heute selbstverständlich gegen externe Bedrohungen wie Viren, Wurmer, Trojaner und fremde Zugriffe geschützt. Dabei stehen Investitionen für Firewalls und Security-Gateway-Systeme im Vordergrund. Der Schutz gegen interne Bedrohungen im Netz steht dagegen nicht selten nur in der zweiten Reihe.

Ein hochverfügbares Rechnernetzwerk als Kommunikationsinfrastruktur ist heute die notwendige Voraussetzung für einen reibungslosen Ablauf der Geschäftsprozesse. Die lokalen Netze basieren dabei auf Ethernet und TCP/IP und sind Verbindungsglied für PCs und Server respektive für die Applikationen und deren Zugriff auf die Daten(banken). Dieser Zugriff auf solche Daten sollte jedoch reglementiert sein, insbesondere sind unberechtigte Zugriffe zu verhindern. Den externen Schutz übernehmen Firewalls und Security-Gateway-Systeme. Des Weiteren helfen dabei Intrusion-Detection- (IDS), Intrusion-Prevention- (IPS) und Virenschutzsysteme, die jedoch für einen internen Schutz nicht immer ausreichend sind. Dabei entwickeln sich Gefahr und Schaden von internen Angriffen zunehmend, korrelierend mit der Digitalisierung der Prozesse.

Betroffen sind alle Unternehmen und Organisationen, die sensible Daten verarbeiten. Im Prinzip kann jeder, der Zugang zum Netzwerk hat, interne Angriffe ausführen. Geeignete und leicht zu bedienende Angriffssoftware ist vielfach im Internet verfügbar. Von persönlichen Vorteilen über Wirtschaftsspionage, Neugier, Erpressung, Sabotage und Mobbing bis hin zum Ehrgeiz von „Hobby-Hackern" und Skript-„Kids": An Motiven für Angriffe mangelt es nicht. Nicht zuletzt können Angriffe auch unabsichtlich und durch technische Unwissenheit erfolgen, etwa durch Malware auf „verseuchten" Notebooks von Gästen im Netz.

Bedrohung durch unerlaubte interne Zugriffe

Über das Netzwerk laufen alle möglichen Inhalte in Form von digitalen Daten, zum Beispiel E-Mails mit Dateien oder Tabellen, Inhalte von Datenbanken und Applikationen oder auch Telefonate (VoIP) und Videokonferenzen. Die Kommunikation im Netz verläuft dabei zwischen den digitalen Ressourcen (auf dem Server) und den Endgeräten (PC, Notebook, Drucker, Telefon etc.).

Ein interner Zugang zum Netz ist in der Regel durch zahlreiche Netzwerkanschlüsse (Ports) verfügbar. Das Problem: Auch Fremde können sich unerlaubt einen Zugang zu diesen „Netzeingängen" verschaffen und dann eine Attacke starten. Neben den üblichen Schäden durch Viren, Würmer und Trojaner droht dann noch eine weitere Gefahr. Der Zugang von nicht autorisierten Dritten zur Kommunikation im Netz und die daraus entstehende Bedrohung, Daten abzuhören, zu manipulieren oder umzuleiten.

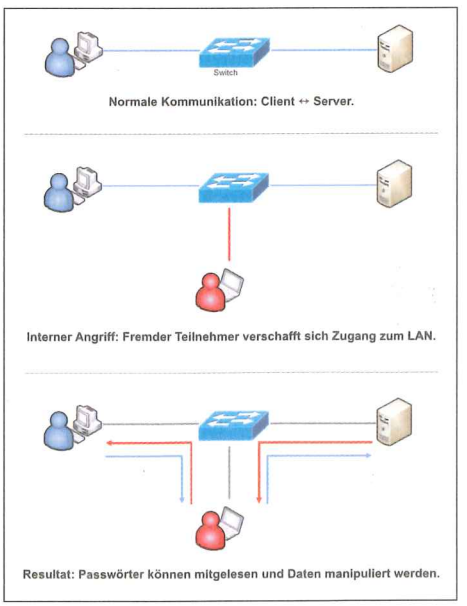
So gab es zum Beispiel den Fall in einer Bankfiliale, wo nach einem Einbruch nichts fehlte. Nur die Fensterscheibe war zerstört. Ein paar Wochen später bemerkte man dann Anomalien in den Zahlungsanweisungen und etwas später auch einen fremden Wireless Access Point unter einem Schreibtisch in der vermeintlich nicht beraubten Filiale.

Die Einbrecher hatten sich per WLAN einen internen Zugang zum Banknetz verschafft. Die Konsequenzen durch solche Angriffe sind natürlich unangenehm und zumeist geschäftsschädigend. Neben Imageschaden, Kosten und Wettbewerbsnachteilen drohen oft auch rechtliche Folgen und Haftungsprobleme.

Bedrohung durch interne Angriffe im Detail

Geplante Angriffe auf den OSI-Layern 3 bis 7 sind eher schwierig, denn sie erfordern ein tiefes Know-how und detaillierte Hintergrundinformationen. Zudem besteht ein Risiko einer Enttarnung (IDS/IPS), denn es entstehen Spuren. Im OSI Layer 2 dagegen ist ein Angriff leicht durchführbar und ein tiefes Know-how dabei nicht zwingend erforderlich. Im Prinzip ist nur eine IP-Adresse notwendig und eine der leicht verfügbaren Angriffsapplikationen. Spuren hinterlässt der Täter nicht, sodass kaum ein Risiko der Entdeckung besteht.

Ein Angreifer, der direkten Zugriff auf ein Netzwerk hat, kann eine Vielzahl von Attacken ausfuhren, zum Beispiel ARP-Spoofing/ARP-Poisoning (Man-in-the-Middle), MAC Flooding oder IP- und MAC-Spoo-



Ablauf einer Man-in-the-Middle-Attacke: Die OSI-Schicht 2 ist sensibel.

fing-Angriffe. Mit zu den gefährlichsten Angriffsszenarien zählen die so genannten ARP- und MAC-Spoofing-Attacken.

ARP und MAC

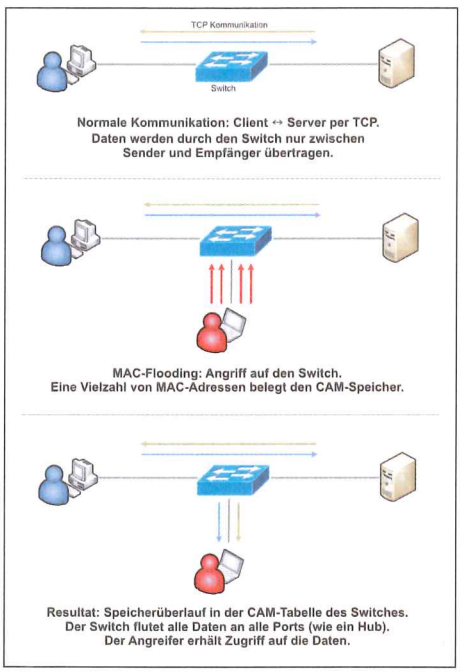
Ein Endgerät im lokalen Ethernet-Netzwerk wird anhand der weltweit eindeutigen (physischen) Adresse seiner Netzwerkkarte angesprochen. Diese Hardwareadresse heißt MAC-Adresse (MAC ≡ Media Access Control). ARP (Address Resolution Protocol) ist ein im Netzwerk notwendig genutztes Protokoll, das die Zuordnung zwischen den Hardwareadressen (MAC) und Protokolladressen (IP) vornimmt. Da ein Sender im Netz oft nur die IP-Adresse des Empfängers kennt, hilft das ARP-Protokoll, die gesuchte MAC-Adresse des Empfängers zu ermitteln. Diese Zuordnungen sind in einer ARP-Tabelle im Endgerät gespeichert, um nicht bei jedem zu sendenden Paket erneut per ARP-Protokoll die Adress-Zuordnung ermitteln zu müssen.

Angriffe laufen so ab, dass die Täter mittels geeigneter Tools gefälschte ARP-Pakete erzeugen und gezielt an andere PCs im gleichen Subnetz senden. Eine besondere Form der ARP-Spoofing-Angriffe sind dabei die so genannten ARP-Poisoning-Angriffe. Dabei werden die ARP-Tabellen von anderen PCs gezielt manipuliert, mit dem Zweck, die Kommunikation zwischen zwei Computern über den Angreifer erfolgen zu lassen. Er ist dann der so genannte „Man-in-the-Middle". Das Bild rechts skizziert diese Vorgehensweise.

Mittels ARP-Spoofing (ARP-Poisoning) ist es somit möglich, Daten abzuhören, Passwörter zu sammeln sowie Daten zu manipulieren, zu blockieren oder umzuleiten. Dies ist oft auch bei verschlüsselten Verbindungen (SSH/SSL) machbar, da die notwendigen Zertifikate nicht immer ausreichend geprüft sind Auch Telefonate (VoIP) lassen sich abhören.

MAC-Spoofing und MAC-Flooding

Mithilfe von geeigneten Tools ist es einem Angreifer möglich, sich gegenüber dem Netz mit einer anderen MAC-Adresse zu „maskieren". Mit Verwendung dieser kopierten MAC-Adresse, dem so genannten MAC-Spoofing, erscheint er wie „verkleidet" im Netz, im Prinzip als jemand anderes, respektive als eine andere Hardware. Dies ist insbesondere bei Anschlüssen von Netzwerkdruckern problematisch. Die Drucker sind wie PCs offizielle Teilnehmer im Netz und ebenfalls durch ihre (weltweit) eindeutige MAC-Adresse identifiziert. Drucker jedoch bieten auch einem fremden Dritten alle notwendigen Informationen zum Netz (IP-Adresse, Gateway etc.), sodass dieser per MAC-Spoofing mit seinem Notebook unerlaubt und „verkleidet als Drucker" Zutritt ins Netz erlangen kann.



Ablauf eines Angriffs per MAC-Flooding.

MAC-Flooding-Angriffe haben das Ziel, die CAM-Tabellen der Switches zum Überlauf zu bringen. In den CAMs (Content Addressable Memory) sind MAC-Switchport-Zuordnungen gespeichert, mit deren Hilfe ein Switch die für eine MAC adressierten Pakete nur auf dem Port weiterleitet, an dem die Empfänger-MAC angeschlossen ist.

Lauft der CAM-Speicher über, ist der Switch gezwungen, alle Daten an alle Ports weiterzuleiten (zu fluten). Der Switch verhält sich dann wie seinerzeit ein Hub und der Angreifer erhält Zugriff auf die Daten. Ein ähnliches Switch-Verhalten kann im Rahmen von Redundanzumschaltungen mit dem Spanning-Tree-Protokoll entstehen. In dessen Umschaltphase flutet der Switch ebenfalls alle Daten an alle Ports. Wie löst man das Problem? Die IT-Abteilung könnte jegliche fremde Hardware vorab analysieren, was jedoch sehr arbeitsaufwändig wäre und zudem ohne Admin-Rechte wenig sinnvoll. Auch Haftungserklärungen bieten keinen effektiven Schutz, ebenso wenig ein Verbot von fremder Hardware.

Die Pflege von statischen ARP-Tabellen wäre ebenfalls schlichtweg zu aufwändig, und die Nutzung von Intrusion-Detection-Systemen ist meist suboptimal, da diese Lösungen in der Regel keine ARP-Angriffe erkennen können. Ebenso sind DHCP-Konfigurationen nur bedingt zur Abwehr von fremden Geräten geeignet, denn sie lassen sich leicht umgehen. Port-Security ist nur schwer administrierbar. Port-Authentifizierung gemäß IEEE 802.1x ist Support-intensiv und zudem dennoch angreifbar.

Die Lücke schließen soll die Lösung Arp-Guard des deutschen Herstellers Internet Sicherheitslösungen (ISL) aus Hagen. Sie arbeitet laut ISL hersteller- und plattformunabhängig und ist beliebig skalierbar. Insbesondere sind keine Investitionen in neue Endgeräte oder Strukturen erforderlich. Die Lösung erkennt aktuelle Bedrohungen und reagiert nur im konkreten Angriffsfall. Zu den Features zählen Network Access Control (NAC), Layer-2 IPS, VLAN- und Netzwerk-Management und Endpoint Security. Eine vollständige Zugangskontrolle auf Layer entsteht laut ISL durch eine MAC-Authentisierung und das Zusammenspiel mit 802.1X, RADIUS, Microsoft AD und/oder Mischformen davon. Das Arp-Guard-Management-System ist als Appliance (Bundle von Hard- und Software) sowie als reine Softwarelösung respektive als VMware-Paket erhältlich. Die Software läuft unter Linux (Red Hat oder CentOS) und unter Windows (nur für Sensoren). Nötig sind ein Management-System, das gleichzeitig auch als Sensor arbeiten kann, sowie eine passende Anzahl von Lizenzen, die mit der Summe der MAC-Adressen im Netz korreliert.

Oliver Lindlar und Mirco Jakuszeit/jos

Oliver Lindlar und Mirco Jakuszeit sind beim Security-Consulting Unternehmen Gordion tätig.