

19.06.08

Von: Thomas Gronenwald

adMERITia: UPnP bietet Angreifern eine Vielzahl an Möglichkeiten ein System zu manipulieren



Wofür steht UPnP?

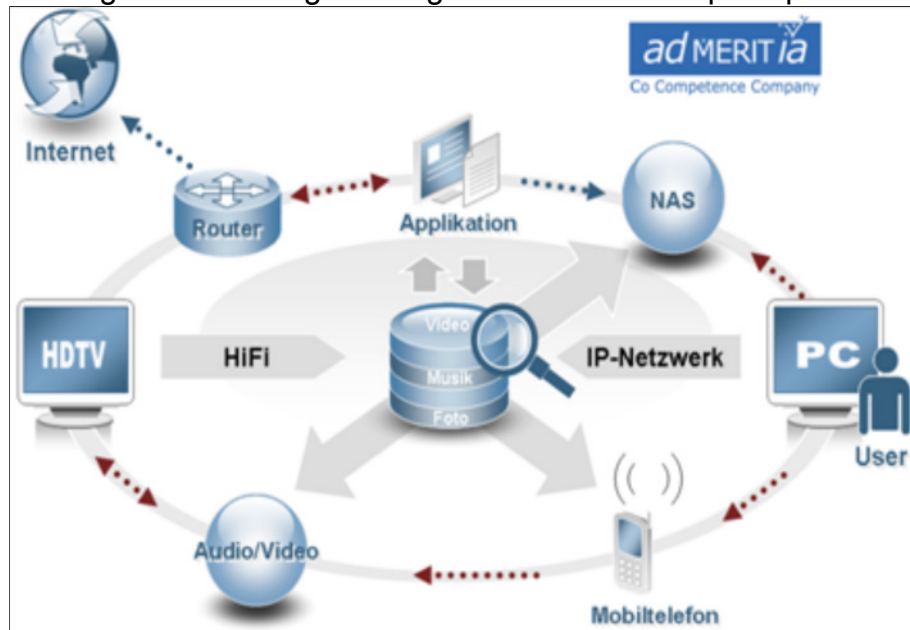
UPnP steht im generellen für Universal Plug and Play und wurde ursprünglich von der Firma Microsoft entwickelt und eingeführt. Heute spezifiziert das UPnP-Forum den UPnP-Standard und entwickelt mithilfe von namhaften Herstellern der Elektronikbranche neue und UPnP-kompatible Geräte.

Die Idee hinter UPnP ist einfach und zugleich interessant. Dennoch ist UPnP häufiger aufgrund bekanntgewordener Schwachstellen in den Schlagzeilen, als den Entwicklern lieb sein mag. Das eigentliche Ziel des UPnP-Protokolls ist es, mediums- und plattformunabhängig die Implementierung von Netzwerkgeräten zu beschleunigen und zu vereinfachen. Genauer gesagt können UPnP-fähige Geräte selbstständig miteinander kommunizieren und benötigte Konfigurationsparameter nahezu eigenständig anpassen. Hinzukommt, dass UPnP eine ideale Kompatibilität mit TCP/IP, UDP, HTTP, XML und anderen Protokollen gewährleistet. Jeder Sicherheits-affine Anwender versteht nun natürlich, was dieses eigenständige Konfigurieren für die Sicherheit eines IT-Verbundes bedeutet: Richtig Am einen Ende gewinnt man an Bequemlichkeit - am anderen Ende verliert man erheblich an Sicherheit.

Eine UPnP-taugliche Applikation in Verbindung mit einem UPnP-fähigen Router erlaubt es etwa, eine Port-Weiterleitung für die Kommunikation mit Webservern völlig eigenständig einzurichten. Auch Schadsoftware wie Malware und Viren nutzen diese Eigenschaften und können so den unerwünschten Zugriff auf Geräte erlangen. Daneben können Angreifer und Malware gleich mehrere bekannte Sicherheitslücken ausnutzen und das Zielsystem so schnell kompromittieren.

Angrenzend öffnen sich dem Angreifer gleich mehrere potenzielle Möglichkeiten ein Gerät zu attackieren. Angefangen bei herkömmlichen und immer beliebter werdenden Phishing-Attacken bei dem der Angreifer versucht typische Angriffsziele wie Zugangsdaten für Banken (Online-Banking) oder Bezahlssysteme (z.B. PayPal) zu erlangen, bis hin zum Öffnen von kritischen Ports zum Einschleusen von Schadsoftware.

Das folgende Bild zeigt das eigentliche Funktionsprinzip von UPnP:



UPnP arbeitet und kommuniziert völlig mediums- und plattformunabhängig, dadurch können sowohl drahtlose- als auch kabelgebunden Netzwerke als Übertragungsmedium genutzt werden. Um die Systeme miteinander zu verbinden, muss lediglich ein Kontrollpunkt im internen LAN verfügbar sein.

Bereits heute gibt es eine Vielzahl an Geräten, die sich UPnP bedienen, darunter zählen beispielsweise Mobiltelefone, HiFi-Geräte, Computer und diverse Netzwerkkomponenten. Schon hier merkt man, welche Kompatibilität nötig ist, um solche Geräte verschiedener Hersteller und Kategorien miteinander zu koppeln. Da bei der Entwicklung jedoch höchste Priorität auf die Interoperabilität von UPnP gelegt wurde, sind Sicherheitsmechanismen dabei leider außen vorgeblieben.

Wie (un-)sicher ist Universal Plug and Play?

Das UPnP-Protokoll beinhaltet standardmäßig keinerlei implementierte Authentifizierungsmechanismen. Daher werden für die Kommunikation zwischen UPnP-Geräten keine Benutzerdaten oder Sicherheitsschlüssel benötigt. Dadurch kann fast jede beliebige Applikation, sei es eine vertrauenswürdige oder eine Schadsoftware Einstellungen an Netzwerkparametern unbemerkt ändern. Hinzukommt, dass die meisten UPnP-Geräte bereits ab Werk standardmäßig im Verbindungsprofil UPnP aktivieren. Die Nutzer dieser Geräte bemerken in den meisten Fällen diese Sicherheitslücke nicht, weil sie UPnP zumeist gar nicht nutzen.

Am einen Ende die Bequemlichkeit am anderen Ende Verlust der Sicherheit

Vielen Anwendern ist eine umfangreiche Netzwerkkonfiguration schlichtweg zu zeitaufwendig und zu kompliziert. Bekanntermaßen bietet UPnP dem Anwender fast grenzenlose Möglichkeiten und einen großen Zeit- und Konfigurationsvorteil, jedoch sollten Anwender ausreichend sensibilisiert sein und mögliche Sicherheitsrisiken kennen.

Welche Möglichkeiten eröffnen sich einem Angreifer?

UPnP bietet Angreifern eine Vielzahl an Möglichkeiten ein System zu manipulieren. Bereits heute gibt es mehrere bekannte Angriffsszenarien. So ist es einem Angreifer beispielsweise möglich, die komplette Kontrolle über bestimmte Router zu erlangen. Dieser Angriff ist dabei sowohl über das LAN als auch über das Internet möglich. Der Angreifer macht sich hierbei bekannter Sicherheitslücken beim Cross-Site-Scripting zunutze. Auch bei einem solchen Szenario ist es dem Angreifer möglich, folgende Parameter und Konfigurationen zu seinen Gunsten zu ändern:

Port-Forwarding um

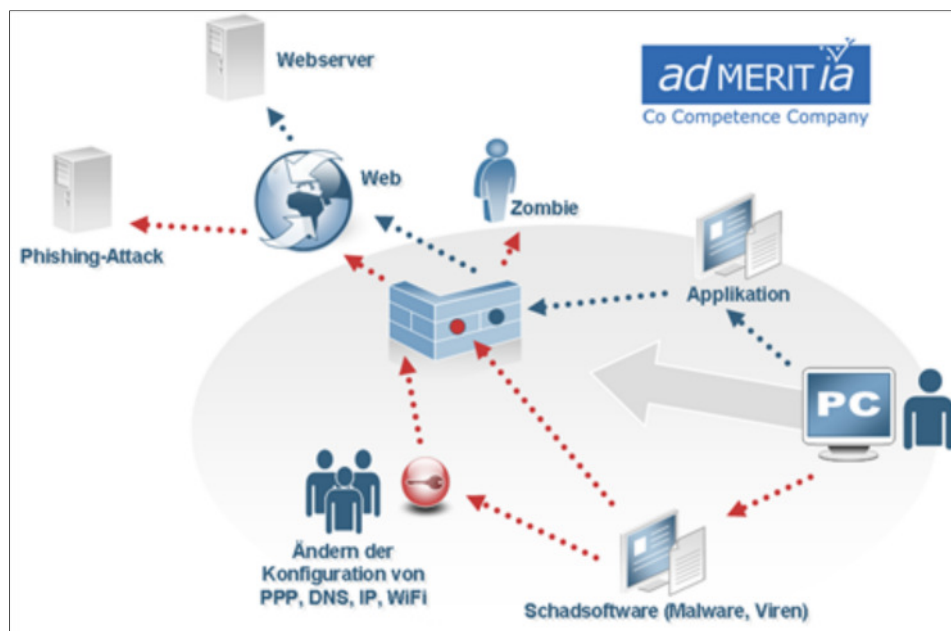
- die interne Administrationsoberfläche von außen verfügbar zu machen
- beliebige Weiterleitungen einzurichten und das System im Nachgang zu übernehmen (Zombie)

Änderung der DNS-Server um

- auf Phishing-Seiten (Online-Banking) umzuleiten
- ungemerkt Malware zu installieren

Änderung von Konfigurationsparametern um

- Usernamen und Passwörter zu manipulieren
- Änderungen an den PPP-Verbindungsdaten vorzunehmen
- IP-Adressen der Router-Interfaces zu ändern
- WiFi-Einstellungen des Routers zu ändern
- Verbindungen zu trennen



Wie lassen sich die Gefahren minimieren? Gibt es UPnP-Sicherheitsvorkehrungen? Welche?

Klar ist, dass man erst einmal die potenziellen Risiken kennen muss, bevor man diese minimieren kann. Sobald diese Risiken transparent und verständlich sind, kann entschieden werden, in welchen Umgebungen und in welchen Konstellationen UPnP genutzt werden kann. Auch auf Seiten der Softwarehersteller macht man sich bereits seit längerem Gedanken um die

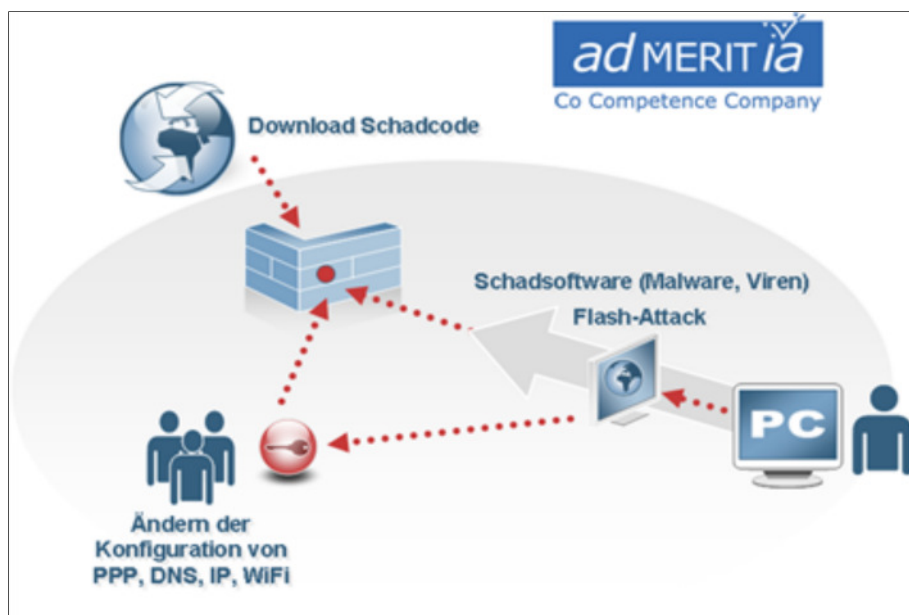
Sicherheit von UPnP. So hat Microsoft bereits für einige Betriebssysteme Best Practices in Bezug auf UPnP veröffentlicht.

Wie bemerke ich einen Angriff?

Einem Angreifer stehen in den meisten Fällen alle Türen offen. Ein Angriff ist meist nicht erkennbar und lässt sich nur schwer reproduzieren. Da zumeist keine UPnP-Aktivitäten protokolliert werden, hinterlässt der Angreifer auch keinerlei Spuren. Der ahnungslose Anwender kämpft meistens nur mit den Auswirkungen eines Angriffs und vermutet erfahrungsgemäß andere Sicherheitslücken hinter einem UPnP-Angriff. Nur zu oft werden für solch einen Angriff die Ursachen bei Anti-Viren oder Firewallkomponenten gesucht.

Kann eine bereits im LAN befindliche Malware sich UPnP bedienen? Mit welchen Auswirkungen?

Generell lässt sich sagen, dass sich nahezu jede Software UPnP bedienen kann. Dabei ist es unwesentlich, ob es sich dabei um eine vertrauenswürdige oder um eine Schadsoftware wie beispielsweise Malware handelt. Da es ohne eine Authentifizierung der Software und Geräte nicht möglich ist, festzustellen ob eine Kommunikation mit UPnP erlaubt ist oder nicht, kann sich Malware genauso der Dienste bedienen wie vertrauenswürdige Applikationen. Eine bekanntgewordene Sicherheitslücke bedient sich so beispielsweise fehlerhafter Flash-Komponenten in einer infizierten und manipulierten Internetseite. So ist es möglich, über einen manipulierten Code in einer Flash-Komponente, Ports zu öffnen und Malware im Netzwerk zu platzieren.



Fazit

Auch bei UPnP gilt es festzuhalten, dass die Sicherheit eines Gesamtsystems immer nur so stark ist wie das schwächste Glied in der Kette. Um die Sicherheit in Bezug auf UPnP zu wahren, empfiehlt es sich jedoch UPnP zu deaktivieren.

Jedem sollte dabei auch klar sein, dass das reine Ausschalten des UPnP-Protokolls ein System noch lange nicht sicher macht. Es muss sichergestellt werden, dass alle potenziellen Sicherheitslücken geschlossen wurden. Lediglich dies verhindert den ungewollten Zugriff auf vorhandene Systeme und Gerätschaften.

Im Endeffekt heißt dies für den Anwender, dass er sicherstellen muss, dass alle Sicherheits- und Betriebssystemkomponenten einwandfrei funktionieren und auf einem aktuellen Patchlevel sind.

Thomas Gronenwald, Security Consultant bei der Firma adMERITia GmbH

www.admeritia.de

- Verwandte Themen
- adMERITia: SCADA-Systeme kommen in sogenannten Prozessdatennetzen (PDN), Prozessnetzen (PZN) oder Prozesssteuerungsnetzen (PSN) zum Einsatz.

Copyright All-About-Security.de / www.all-about-security.de Alle Rechte vorbehalten
Vervielfältigung nur mit Genehmigung von All-About-Security.de