Sichere Fernwartung über das Internet

Implementierung, Skalierbarkeit, Zugriffs- und Datenschutz

DI Günter Obiltschnig
Applied Informatics Software Engineering GmbH
Maria Elend 143
9182 Maria Elend
Austria
guenter.obiltschnig@appinf.com

Einleitung

Bei vielen Netzwerk-basierten Geräten sind webbasierte Benutzerschnittstellen mittlerweile Standard. Mit ihnen werden, von PC, Smart Phone oder Tablet aus, die Geräte über einen Webbrowser konfiguriert, bedient und überwacht. Dank leistungsfähiger Webbrowser, JavaScript und Ajax Programmiertechniken sind webbasierte Benutzerschnittstellen inzwischen sehr leistungsfähig, ansprechend und benutzerfreundlich. Da sie lediglich eine HTTP(S) Verbindung zwischen Webbrowser und dem auf dem Gerät laufenden Webserver benötigen, sind sie sehr gut aus der Ferne nutzbar und stellen somit eine brauchbare technische Basis für Fernwartungszwecke dar. Voraussetzung ist jedoch, dass der Webbrowser eine HTTP Verbindung zum Webserver im Gerät aufbauen kann. Das funktioniert nur, wenn sich das Gerät im selben Netzwerk wie der Webbrowser befindet oder das Gerät direkt mit dem Internet verbunden und über eine öffentliche IP Adresse erreichbar ist. Leider sind diese Voraussetzungen in der Praxis kaum gegeben. Häufig befinden sich Geräte in privaten Netzen hinter NAT Routern oder Firewalls. Selbst für Geräte, die sich in einem mobilen Netz wie GSM/GPRS oder UMTS befinden, werden vom Netzbetreiber oft nur private IP Adressen vergeben (Carrier-grade NAT). Damit ist es zwar für das Gerät möglich das Internet zu erreichen; umgekehrt kann aber das Gerät nicht direkt über das Internet angesprochen werden, da ein netzinterner NAT Router oder eine Firewall den Zugriff verhindern. Auch IPv6 wird diese Situation nicht wesentlich ändern. Zwar könnte jedes Gerät über eine eindeutige IPv6 Adresse im Internet erreichbar sein. Auf die Firewall im Router wird man jedoch gerade deswegen kaum verzichten wollen.

Port Forwarding und Virtual Private Networks (VPN) sind bekannte technische Möglichkeiten des Internet-basierten Fernzugriffs auf Geräte. Doch beide Varianten sind für den Einsatz in vernetzten Geräten nur bedingt geeignet, in der Umsetzung relativ komplex, und, im Fall von Port Forwarding, ein signifikantes Sicherheitsrisiko. Eine weitere Variante ist der Einsatz sogenannter Relay Services wie my-devices.net [1] oder Yaler [2]. Die einzelnen Technologien mit ihren Eigenschaften bezüglich Implementierbarkeit, Skalierbarkeit, sowie Zugriffs- und Datenschutz werden später noch näher beschrieben.

Fernwartungsszenarien

Je nach Art des Fernwartungsszenarios werden unterschiedliche Anforderungen an eine Fernwartungslösung gestellt. Folgende Szenarien können unterschieden werden:

- Fernzugriff durch den Gerätehersteller zu Wartungs- und Supportzwecken.
- Fernzugriff durch Servicepartner des Geräteherstellers zu Wartungs- und Supportzwecken.
- Fernzugriff durch den Geräteeigentümer, bzw. Benutzer. Dies inkludiert, speziell in Bereichen wie der Heimautomatisierung, auch den Fernzugriff per Smartphone oder Tablet App.

Diese drei Szenarien stellen unterschiedliche Anforderungen an die Fernwartungstechnologie, speziell im Hinblick auf die Verwaltung der Benutzer und deren Zugriffsmöglichkeiten, bzw. Zugriffsberechtigungen.

Verbreitet, aber unsicher: Port Forwarding und Dynamic DNS

Port Forwarding stellt die einfachste Möglichkeit dar, den Zugriff auf einen bestimmten TCP Port (z. B. Port 80 des Webservers) eines Gerätes vom Internet aus zu erlauben. Zu diesem Zweck wird der Internet Router in dessen lokalem Netz sich das Gerät befindet so konfiguriert, dass ein bestimmter externer (zum Internet offener) Port des Routers direkt zum einem bestimmten Port des Gerätes weitergeleitet wird. Die Portnummern können dabei unterschiedlich sein. Betreibt das Gerät den Webserver wie üblich auf Port 80, kann z. B. der externe Port 8080 des Routers zum Port 80 des Gerätes weitergeleitet werden. Kennt man nun die externe IP Adresse des Routers, (z. B. 213.162.68.3) so kann über die URL http://213.162.68.3:8080 auf den Webserver des Gerätes zugegriffen werden. Bei mehreren Geräten muss jedem Gerät eine eindeutige externe Portnummer zugewiesen werden. Das Port Forwarding am Router selbst kann entweder durch den Benutzer selbst eingerichtet werden (vorausgesetzt, der Benutzer verfügt über die erforderlichen Kenntnisse, wovon in der Praxis nicht unbedingt ausgegangen werden kann), oder das Gerät selbst kann über Protokolle wie UPnP IGD oder NAT-PMP den Router entsprechend konfigurieren, sofern der Router dies unterstützt, bzw. erlaubt.

Das technische Problem bei diesem Ansatz ist, dass die externe IP Adresse des Routers nicht unbedingt fix sein muss. In den meisten Fällen wird die Adresse vom Netzwerkanbieter dynamisch vergeben und kann sich daher jederzeit ändern. Somit muss man, um auf das Gerät zugreifen zu können, ständig die aktuelle externe IP Adresse des Routers kennen. Dieses Problem lässt sich über Dynamic DNS in den Griff bekommen. Es gibt Anbieter spezieller DNS Services (z. B. Dyn.com), die es erlauben, die einem Domainnamen zugewiesene IP Adresse jederzeit über eine Programmierschnittstelle zu ändern. Auf dem Router (oder dem Gerät) sorgt dann der sogenannte DynDNS Client dafür, dass dem DNS Dienst laufend die aktuelle externe IP Adresse mitgeteilt wird. Damit kann dann den Webserver des Gerätes über eine URL wie z. B. http://meingeraet.dyndns.org:8080 erreichen.

Das eigentliche Problem von Port Forwarding und Dynamic DNS ist jedoch, dass jeder der die IP Adresse, bzw. die URL des Gerätes kennt, auf dieses zugreifen kann. Der Webserver des Gerätes sollte zwar den Zugriff über Benutzername und Passwort absichern, die Erfahrung zeigt aber, dass die vom Hersteller festgelegten Standardpasswörter in den meisten Fällen erstens unsicher sind und zweitens vom

Benutzer selten geändert werden, oder dass auch gar kein effektiver Passwortschutz vorgesehen ist. Programmierfehler, die ein Umgehen eines eventuell vorhandenen Passwortschutzes einfach möglich machen tun ein Übriges. Ein gutes Beispiel ist die im Frühjahr 2013 bekannt gewordene Sicherheitslücke im Systemregler eines bekannten deutschen Herstellers von Blockheizkraftwerken [3].

Nicht außer acht zu lassen ist auch die Möglichkeit, ein üblicherweise in seinen Rechenressourcen eingeschränktes Embedded System außer Funktion zu setzen, in dem der Webserver mit gezielten Anfragen aus dem Internet überlastet wird. Anders als bei sogenannten Denial-of-Service Angriffe auf „richtige“ Webserver reicht dazu mitunter ein einzelner PC aus. Es gibt mittlerweise Suchmaschinen wie z. B. Shodan [4], die es ermöglichen, gezielt und automatisiert nach bestimmten Gerätetypen zu suchen. Mögliche Bedrohungsszenarien kann man sich leicht vorstellen.

All das macht Port Forwarding zu einer vollkommen ungeeigneten, genau genommen grob fahrlässigen, Möglichkeit, einen Fernwartungszugang zu einem Gerät herzustellen.

Die IT Lösung: Virtual Private Networks

Virtual Private Networks (VPN) stellen eine etablierte Möglichkeit dar, entfernte Systeme über eine sichere, verschlüsselte Verbindung über das Internet in ein internes Firmennetzwerk zu integrieren. Eine typische Anwendung ist der Zugriff auf das Firmennetzwerk von einem Heimarbeiter PC aus. Auch im Automatisierungsbereich wird VPN zunehmend zu Fernwartungszwecken eingesetzt. Viele Hersteller bieten zu diesem Zweck spezielle VPN Router an, die ein Gerät per ASDL oder mobiler Internetverbindung an ein Firmennetzwerk anbinden können. Die VPN Software kann alternativ auch direkt im Gerät selbst implementiert sein. Dabei kommen standardisierte Protokolle, wie z. B. Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), IPSec Tunneling oder OpenVPN zum Einsatz. Aus Zugriffs- und Datenschutz Sicht ist VPN grundsätzlich sicher, abgesehen von bekannten Sicherheitslücken im PPTP. Es wird allerdings eine entsprechende Netzwerk-Infrastruktur (VPN Server) benötigt, die je nach Anzahl der anzubindenden Geräte recht aufwändig sein kann. Weiters ist zu beachten, dass sich alle an ein VPN angebunden Geräte im selben Netzwerk befinden. Gelingt es in das VPN einzudringen (in dem man z. B. im einfachsten Fall das an den VPN Router angeschlossene Gerät durch einen PC ersetzt), hat man automatisch Zugriff auf alle im Netzwerk befindlichen Geräte. Für Anwendungen, wo sich die anzubinden Geräte in unsicheren Bereichen befinden (z. B. in Privathaushalten) muss über zusätzliche Maßnahmen am VPN Server (z. B. entsprechend konfigurierte Firewall) der Zugriff auf andere Systeme im VPN verhindert werden.

Was sich über VPN jedoch nicht einfach realisieren lässt, ist der Fernzugriff per Smartphone App auf das Gerät, außer das Smartphone wird ebenfalls ins VPN eingebunden Dies ist jedoch z. B. bei Geräten für Privatanwender (Heimautomatisierung), nicht praktikabel. Hier wird ein weiterer Server benötigt, welcher über das Internet erreichbar ist, und welcher die Anfragen der Smartphone App nach erfolgter Authentifizierung und Autorisierung an das im VPN befindliche Gerät weiterleitet.

Aus Sicht der Skalierbarkeit eignen sich VPN Lösungen für bis zu mehreren 10.000 Geräten, wobei ein einzelner VPN Server üblicherweise mehrere 1000 gleichzeitige Geräteverbindungen bedienen kann. Bei einer größeren Anzahl an Geräten müssen

mehrere VPN Server zusammengeschaltet werden, außerdem steigen die Anforderungen an die Netzwerkinfrastruktur, da jedes Gerät im VPN Netz eine eindeutige IP Adresse benötigt.

Bereit für die Cloud: Relay Services

Relay Services wie z. B. my-devices.net oder Yaler stellen einen guten Kompromiss zwischen Port Forwarding und VPN dar. Die Funktionsweise dieser Systeme ist so, dass das Gerät eine verschlüsselte Tunnel-Verbindung zum Relay Server (auch Reflector Server genannt) aufbaut. Über diese Verbindung sendet der Relay Server dann HTTP Anfragen an den Webserver des Gerätes. Soll auf das Gerät zu Fernwartungszwecken zugegriffen werden, erfolgt dies immer indirekt über den Relay Server. Der Relay Server übernimmt die Authentifizierung und Autorisierung der HTTP Anfragen und leitet sie an das Gerät weiter. Da das Gerät von sich aus die Verbindung zum Relay Server aufbaut kann jeglicher Zugriff auf das Gerät von außerhalb ausschließlich über den Relay Server erfolgen. Je nach Relay Server können neben HTTP noch anderen Protokolle (z. B. SSH) unterstützt werden. Ein großer Vorteil dieses Ansatzes ist, dass ein Relay Server gut als Cloud Service betrieben werden kann. Eine direkte Integration ins Unternehmensnetz ist nicht unbedingt notwendig. Über bekannte Standard-Lastverteilungsmechanismen kann fast beliebig skaliert werden. So können auch mehr als 100.000 Geräte gleichzeitig angebunden werden. Darüber hinaus erlaubt es z. B. my-devices.net, jedes Gerät über einen eindeutigen Domainnamen anzusprechen. An einen my-devices.net Reflector Server angebundene Geräte sind daher wie jeder normale Webserver im Internet über eine eindeutige URL ansprechbar (z. B. https://meingeraet.my-devices.net). Da aber jeder Zugriff über den Reflector Server läuft, sind die Geräte sowohl vor unberechtigtem Zugriff, als auch vor Denial-of-Service Attacken ausreichend geschützt. Auch der Fernzugriff per Smartphone App ist problemlos möglich. Zu diesem Zweck stellt das Gerät üblicherweise REST Webservices zur Verfügung die von der Smartphone App über HTTPS aufgerufen werden.

Zusammenfassung

Virtual Private Networks und Relay Services wie my-devices.net sind geeignete und sichere Technologien um den Zugriff auf ein Gerät zu Fernwartungszwecken zu realisieren. Je nach Anwendungsbereich weisen die beiden Technologien unterschiedliche Vorteile auf. Soll der Fernzugriff auf ein System ausschließlich aus einem Firmennetzwerk heraus erfolgen (z. B. durch den Hersteller oder Eigentümer des Systems), ist eine VPN Lösung eine geeignete Wahl. Soll der Zugriff jedoch einem weiteren Personenkreis erlaubt werden (z. B. externe Servicedienstleister), oder soll auch z. B. ein Privatanwender selbst aus der Ferne per Webbrowser oder Smartphone App auf sein Gerät zugreifen können, so ist ein Relay Service wie my-devices.net eine bessere Wahl. Port Forwarding und Dynamic DNS stellen jedoch aufgrund des mangelnden Zugriffschutzes keine geeignete Möglichkeit des Fernzugriffes dar.

Referenzen

[1] http://my-devices.net

[2] http://yaler.net

[3] http://www.bhkw-infothek.de/nachrichten/18555/2013-04-15-kritische-sicherheitslucke-ermoglicht-fremdzugriff-auf-systemregler-des-vaillant-ecopower-1-0/

[4] http://www.shodanhq.com

Zum Autor

Günter Obiltschnig ist Geschäftsführer der Applied Informatics Software Engineering GmbH, einem Software-Unternehmen spezialisiert auf C++ Frameworks für netzwerk-basierte Systeme. Er ist außerdem Gründer und leitender Entwickler des Open Source Projektes POCO C++ Libraries. Günter Obiltschnig entwickelt seit über 20 Jahren professionell Software für verschiedenste Systeme – von verteilten Unternehmensapplikationen bis zu Embedded Systemen, hauptsächlich in C++. Als Referent ist er regelmäßig auf verschiedenen internationalen Konferenzen wie z. B. dem ESE Kongress und der Embedded World vertreten.