Netzwerkzugangskontrolle für Energie- und andere Versorger

Höhere Verfügbarkeit durch NAC-Lösungen auf SNMP-Basis

Betreiber von Energienetzen versprechen ihren Kunden, dass die Stromversorgung maximal 32 Sekunden im Jahr ausfällt. Sind die Energieversorger jedoch von ihren IT-Prozessen abhängig, ist dieses Versprechen oft reine Utopie – jedenfalls wenn Produktions- und Büronetze durch NAC-Lösungen auf Basis des 802.1X-Standards getrennt werden. Eine Alternative bietet die noch weniger bekannte NAC-Technologie SNMP.

Von Dr. Andreas Rieke, ISL Internet Sicherheitslösungen GmbH

In seinem Buch „Blackout" beschreibt Marc Elsberg eindrucksvoll, wie sich der Ausfall der Stromversorgung über einen längeren Zeitraum auswirkt. Ob das Buch Inspiration für den Gesetzgeber war, die Betreiber von kritischen Infrastrukturen und besonders die Energieversorger stärker in die Pflicht zu nehmen, bleibt Spekulation. Fakt ist: Die Pflicht zu mehr Sicherheit ist im Energiewirtschaftsgesetz (EnWG) und im neuen IT-Sicherheitsgesetz klar geregelt. Ein angemessener Schutz liegt laut EnWG vor, wenn die dort definierten Sicherheitsanforderungen umgesetzt und eingehalten werden und dies dokumentiert ist. Alle weiteren Versorger (Gas, Wasser, usw.) sind nach einer Übergangsfrist von 18 Monaten ebenso betroffen wie die zuvor erwähnten Energieversorger. Wer sich so angemessen schützt, haftet dann auch nicht mehr für Schäden, die beispielsweise aus Versorgungsengpässen entstehen.

Dass sich Betreiber von Energienetzen vor Schadenersatzforderungen durch Versorgungsengpässe schützen müssen, zeigt folgendes Beispiel. So war bei analoger Telefonie keine Stromversorgung im Haus des Endverbrauchers erforderlich. Mit der Umstellung auf Voice over IP (VoIP) ändert sich das jedoch: Die dafür notwendige Hardware, wie DSL-Router, benötigen eine kontinuierliche Stromversorgung. Fällt diese aus, funktioniert auch das Telefon nicht mehr – kommt es nun zu einem medizinischen Problem, lässt sich kein Notruf mehr absetzen. Die Haftung für den Versorger ist in diesem Fall laut EnWG nur ausgeschlossen, wenn der Netzbetreiber den vorgeschriebenen Sicherheitskatalog umgesetzt hat. Anderenfalls sind Schadenersatzforderungen des Kunden möglich.

Die gesetzliche Basis

Der Katalog von Sicherheitsanforderungen im EnWG beinhaltet im Wesentlichen einen Verweis auf die seit längerem eingeführte Norm DIN ISO/IEC 27001. Sie beschreibt ein Informationssicherheits-Managementsystem (ISMS), das Vorgaben für viele Bereiche der IT-Sicherheit enthält. Unter anderem sind darin deutliche Anforderungen auf ein System zur Zugangskontrolle zum Netzwerk (Network Access Control - NAC) enthalten:

DIN ISO/IEC 27001 - A.9.1.2

„Zugang zu Netzwerken und Netzwerkdiensten: Benutzer haben ausschließlich Zugang zu denjenigen Netzwerken und Netzwerkdiensten, zu deren Nutzung sie ausdrücklich befugt sind."

DIN ISO/IEC 27001 - A.13.1

„Netzwerksicherheitsmanagement: Der Schutz von Informationen in Netzwerken und unterstützenden informationsverarbeitenden Einrichtungen ist sichergestellt."

DIN ISO/IEC 27001 - A.13.1.3

„Trennung in Netzwerken: Informationsdienste, Benutzer und Informationssysteme werden in Netzwerken gruppenweise voneinander getrennt gehalten."

DIN ISO/IEC 27002- A 13.1.1

„Netzwerkkontrollen: Netzwerke sollen so verwaltet und kontrolliert werden, dass die Informationen in Systemen und Anwendungen geschützt sind." Umsetzungshinweise finden sich in „f) Die Systeme im Netzwerk sollten authentifiziert werden" und „g) Die Systemverbindung zum Netzwerk sollte eingeschränkt sein".

802.1X und seine Tücken

Speziell Energieversorger stehen bei der Umsetzung der beschriebenen Maßnahmen jedoch vor einer Herausforderung, beson-

ders wenn auf den internationalen Standard 802.1X gesetzt wird. So sind beispielsweise Endgeräte, wie Spannungssensoren, Videoüberwachungs-Kameras oder SCADA-Systeme, die Energieversorger in ihren Umspannwerken oder Kraftwerken benutzen, nicht für das Protokoll 802.1X ausgelegt. Auch speziell für raue Umgebungsbedingungen konstruierte Industrieswitche unterstützen das Protokoll oft nicht. Hinzu kommt der Irrglaube, ein Zertifikatsbasierendes 802.1X sei sicher, weil es mit kryptografischen Verfahren arbeitet. Das trifft vielleicht im WLAN zu, im LAN ist das jedoch nicht der Fall. Hier kann selbst ein Anfänger in wenigen Minuten Zugriff zum Netz bekommen (Session-Hijacking).

Die beschriebenen Punkte sind im Prinzip schon K.-o.-Kriterien für die Einführung einer NAC-Lösung auf Basis des Protokolls 802.1X. Es kommt jedoch noch hinzu, dass bei der Nutzung von 802.1X ein Ausfall der NAC-Lösung in der Regel den Gesamtausfall des Netzwerkes zur Folge hat.

Die Alternative SNMP

Eine Alternative bietet hier die meist noch unbekannte NAC-Technologie Simple Network Management Protocol (SNMP). Solche NAC-Lösungen durchsuchen periodisch das Netzwerk mittels SNMP-Zugriffe auf vorhandene Router und Switches nach unbekannten Endgeräten. Werden solche Endgeräte gefunden, alarmiert die NAC-Lösung die verantwortliche Person und leitet Gegenmaßnahmen ein, wie zum Beispiel die Abschaltung von Ports. Weitere Vorteile der SNMP-Technologie sind:

_ Bei einem Ausfall der NAC-Lösung haben weiterhin alle Systeme uneingeschränkten Zugriff auf das Netzwerk. Die Energieversorgung bleibt somit weiterhin gewährleistet. Die NAC-Verfügbarkeit lässt sich zudem durch Cluster erhöhen.

_ Die im Standard beschriebenen und von so gut wie allen Switchherstellern implementieren SNMP-Traps erreichen schnelle Reaktionen – in der Regel innerhalb von 200 bis 300 Millisekunden.

_ Die Lösung kann aktiv arbeiten und Ports abschalten oder alternativ bei einer passiven Arbeitsweise lediglich per E-Mail alarmieren – die Entscheidung liegt beim Betreiber.

_ Die per SNMP zur Identifizierung verwendeten MAC-Adressen lassen sich relativ leicht fälschen. Lösungen mit kryptografischem Fingerprinting erhöhen das Sicherheitsniveau deutlich.

_ SNMP-Lösungen sind wirtschaftlich: Das Verhältnis von Gesamtkosten (Produktkosten, Personalkosten, Betriebskosten über mehrere Jahre) zum Nutzen (Sicherheit des Verfahrens sowie Mehrwerte wie Monitoring) verdeutlicht die Vorteile der Technologie.

Fazit

Energieversorger sehen sich weitreichenden Veränderungen ausgesetzt. Das Zusammenwachsen von IT- und Stromnetzen sowie gesetzliche Rahmenbedingungen fordern mehr Sicherheit. Die Herausforderung dabei ist, dass die geringere Verfügbarkeit der IT keine Auswirkung auf die Verfügbarkeit der Energieversorgung haben darf. Die notwendigen Technologien sind dafür jedoch am Markt vorhanden, wie beispielsweise die in Deutschland entwickelte NAC-Lösung ARP-GUARD. (www.arp-guard.com). Bei der Auswahl einer NAC-Lösung sollte im Vordergrund stehen, dass durch kryptografisches Fingerprinting ein höheres Sicherheitsniveau erreicht wird.