ANWENDERBERICHT
ENERGIESÜDWEST

macmon
nac intelligent einfach

NAC-Lösung Ganzheitlicher Schutz für kritische Infrastruktur – EnergieSüdwest Netz setzt auf macmon für ISMS

Die EnergieSüdwest Netz GmbH erfüllt mit macmon einen wichtigen Teil der KRITIS-Auflagen und optimiert gleichzeitig die Verwaltung des gesamten Netzwerks.

EnergieSüdwest | Netz GmbH

Die EnergieSüdwest Netz GmbH ist ein Tochterunternehmen der EnergieSüdwest AG und wurde am 15.06.2007 mit Sitz in Landau in der Pfalz gegründet. Sie bewirtschaftet die Strom-, Gas-, Wasser- und Fernwärmeinfrastruktur in und um Landau mit über 60 Mitarbeitern. Hierzu gehören neben Planung, Bau und Betrieb der Versorgungsnetze, das Regulierungsmanagement, die Netzabrechnung, die Durchführung von Kundenwechselprozessen, das Pflegen von Vertragsbeziehungen in den liberalisierten Märkten, der Messstellenbetrieb, uvm. Der Standort hat ca. 100 Netzwerkgeräte im Einsatz.

Ein ganzheitlicher Ansatz ist nötig

Als Energieanbieter fällt die EnergieSüdwest Netz GmbH in den Bereich der kritischen Infrastrukturen (KRITIS) des seit 2015 geltenden IT-Sicherheitsgesetzes, für die seit Mai 2016 der erste Teil der KRITIS-Verordnung gilt. Demnach müssen von den betroffenen Organisationen spezielle Maßnahmen umgesetzt werden, um die Verfügbarkeit und Sicherheit ihrer IT-Systeme zu sichern. Darunter fällt auch das sogenannte ISMS wie im „IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz" (Stand August 2015) beschrieben:

„Neben den überzeugenden Funktionalitäten, den kurzen Kommunikationswegen und der kompetenten, unkomplizierten Unterstützung von Seiten macmon und BWG, war die BSI-Zertifizierung der Lösung eines der Hauptargumente für unsere Entscheidung."

Thomas Gallion, EnergieSüdwest Netz GmbH

„Zur Gewährleistung eines angemessenen Sicherheitsniveaus für TK- und EDV-Systeme, die für einen sicheren Netzbetrieb notwendig sind, ist die bloße Umsetzung von Einzelmaßnahmen, wie zum Beispiel der Einsatz von Antivirensoftware, Firewalls usw. nicht ausreichend. Zur Erreichung der Schutzziele ist stattdessen ein ganzheitlicher Ansatz nötig, der kontinuierlich auf Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf anzupassen ist. Einen solchen ganzheitlichen Ansatz stellt ein sog. Informationssicherheits-Managementsystem (ISMS) dar."

Durch die immer weiter wachsende Anzahl an netzfähigen Geräten, wie Drucker und IP-Telefone innerhalb des Unternehmensnetzes, steigen auch die Angriffsflächen für Cyberattacken. Daher wird der ganzheitliche Schutz dieses Netzes durch Netzwerkzugangskontrolle (Network Access Control, NAC) einer der wichtigsten Maßnahmen zur Einrichtung eines ISMS.

Wenig Aufwand und leistungsstarke Funktionen

Um den Schutz des Netzwerks im Rahmen eines ISMS auf Grundlage des IT-Sicherheitskatalogs abzubilden, suchte EnergieSüdwest Netz nach einem Partner, der die umfassende Absicherung des Netzwerks mit möglichst wenig Aufwand realisieren kann. Während der ausführlichen Marktrecherche kristallisierte sich die NAC-Lösung von macmon, die den Verantwortlichen durch die BWG Systemhaus Gruppe vorgestellt wurde, als Topkandidat heraus.
Zur ausführlichen Evaluation wurde macmon vorerst in einer eingeschränkten Produktivumgebung eingesetzt. Hier stach die leistungsstarke Topologieerkennung mit LLDP und CDP und der hohe Grad an Automatisierung der Lösung positiv heraus.
Sie macht auch komplexe oder weit verzweigte Netzwerke rasch sichtbar und erleichtert das Management des gesamten Netzwerks erheblich.
Da macmon ein deutscher Hersteller mit Sitz in Berlin ist und die Lösung vom BSI mit dem IT- Sicherheits-

Stand: 01/2017

zertifikat ausgezeichnet ist, waren zudem Bedenken hinsichtlich der Sicherheit und Richtlinienkonformität hinfällig. Daher fiel die Entscheidung letztendlich auf das Premium Bundle von macmon, das NAC, Advanced Security, VLAN Manager, Guest Service, IEEE 802.1X, Grafische Topologie und umfangreiche Mechanismen, um den Compliance-/Sicherheitsstatus von Endgeräten zu prüfen.

EnergieSüdwest Netz betreibt macmon als Cluster auf physikalischen Appliances. In den überwachten Bereichen kommen u.a. Industrieswitches des Herstellers Microsense zum Einsatz. Um das ISMS vollständig abzubilden, setzt die ESW Netz neben macmon NAC zusätzliche Sicherheitslösungen wie unter anderem eine Firewall und zwei Antiviren-Lösungen ein. Die Lösung wurde mit Unterstützung durch den Partner BWG und macmon selbst implementiert.

Maximale Sicherheit und Kontrolle bei minimalem Managementaufwand

Mit macmon können die fünf für die Netzwerktechnik zuständigen Mitarbeiter bei EnergieSüdwest Netz GmbH ihr Netzwerk effizient und umfassend überwachen, während sie sich voll auf ihre Kernaufgaben, die außerhalb der IT liegen, konzentrieren.
Das Netzwerk der ESW Netz GmbH ist relativ wenig Fluktuation ausgesetzt und der Großteil der angeschlossenen Geräte arbeitet an weit verteilten Standorten autonom. Daher liegt die Hauptaufgabe von macmon in der lückenlosen Echtzeitüberwachung des gesamten Netzes. Die SNMP-basierte Lösung arbeitet hardwareunabhängig, sodass keine „blinden Flecken", wie bei Appliance- oder Client-basierten Ansätzen, entstehen können.

Betreten neue Endgeräte das Netzwerk an Switches bzw. Interfaces mit falscher VLAN-Konfiguration, werden sie durch die situationseffektive VLAN-Auswahl automatisch und dynamisch in das für die Situation genau richtige VLAN verschoben, ohne dass dafür manuell eine Regel geschrieben werden muss. Damit wird zum einen das Ausmaß und die Komplexität des Regelwerks selbst

reduziert und zum anderen der Administrationsaufwand extrem minimiert. Berührungspunkte mit der Lösung, die manuelles Eingreifen erfordern, gibt es so nur noch, wenn ein unbefugter Zugriff erkannt und automatisch abgesichert wurde. Für die Zukunft ist die Einführung der Authentifizierung von Gastgeräten – z.B. Notebooks von Mitarbeitern – via 802.1X über einen RADIUS-Server geplant. Diese Funktion ist bereits in macmon enthalten und auch Mischbetrieb aus SNMP und 802.1X mit Echtzeitüberwachung ist möglich.

> *„Entscheidend war für uns die Hauptfunktion Network Access Control zur Identifizierung nicht autorisierter Geräte. Sie arbeitet äußerst zuverlässig, so dass Eindringlinge im Netzwerk jederzeit sofort erkannt, automatisch in einem VLAN isoliert und die Administratoren umgehend informiert werden. So erfüllen wir einen zentralen Teil des ganzheitlichen Ansatzes des IT-Sicherheitsgesetzes."*
>
> **Thomas Gallion,** EnergieSüdwest Netz GmbH

Für Beratung und Support stehen macmon und seine Consultingpartner zudem stets bereit. Die Servicemitarbeiter des Herstellers befinden sich alle direkt am Unternehmenssitz in Berlin, sodass Unterstützung und Problemlösung immer schnell und kompetent bereitgestellt werden können.

FAZIT:

Mit der Implementierung von macmon erfüllt EnergieSüdwest Netz einen wichtigen Teil der Vorgaben eines Informationssicherheits-Managementsystems für kritische Infrastrukturen. Zudem erleichtert die Lösung die Verwaltung und Überwachung des gesamten Netzwerks erheblich während bestehende Investitionen durch die Hardwareunabhängigkeit geschützt werden konnten. Auch langfristig geplante Entwicklungen sind von den Funktionen in macmon NAC abgedeckt, sodass das Netzwerk der ESW Netz GmbH zukunftssicher geschützt ist.

Kontakt macmon secure GmbH | Alte Jakobstraße 79-80 | 10179 Berlin | Tel.: +49 30 2325777-0 | nac@macmon.eu | www.macmon.eu

Stand: 01/2017