mdexExperts - Zertifizierte Sicherheit als Service

IT-Sicherheitsanforderungen gemäß ISO 27001

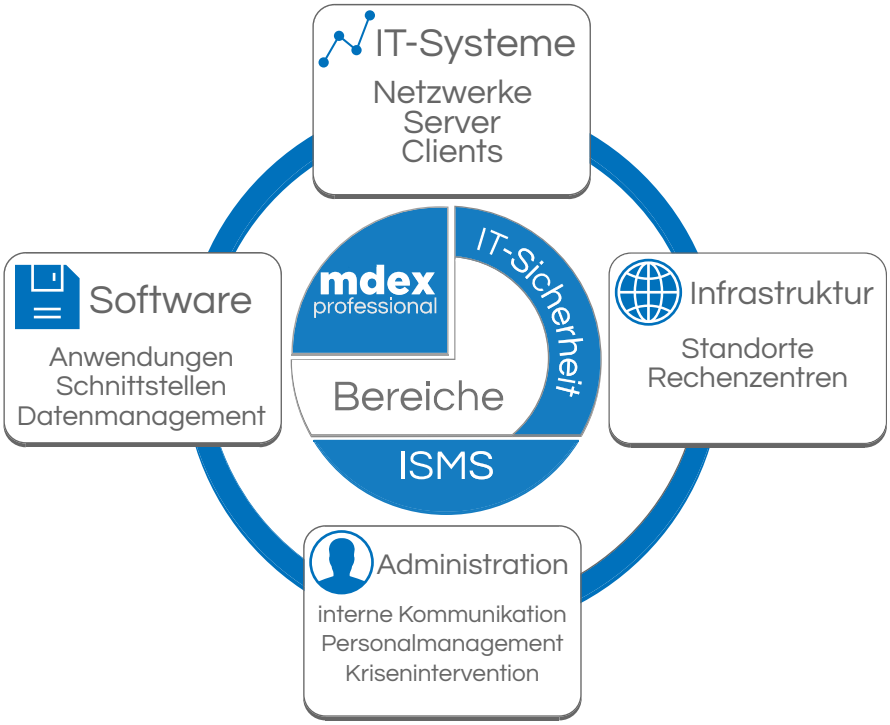

Abbildung 1: mdex ISO 27001 ISMS

Ihr Ansprechpartner

mdexExpert Timo Ross
Leiter Produktmanagement/
Marketing

Energieversorger müssen in ihren Netzwerken unterschiedlichste Geräte und Leitstellen vernetzen – und zwar so, dass diese Lösungen spätestens am 31.01.2018 den Anforderungen des IT-Sicherheitskatalogs der BNetzA entsprechen. Neben den formalen Anforderungen aus diesem Katalog ist die sichere Anbindung von Anlagen in diesen heterogenen Netzen die größe Herausforderung.

Nach dem Inkrafttreten des IT-Sicherheitsgesetzes tickt die Uhr: Stadtwerke und andere Energieunternehmen sind als Anbieter kritischer Infrastrukturen gefordert. Binnen zwei Jahren müssen sie nachweisen, dass die von ihnen betriebenen Technologien sicher im Sinne des IT-Sicherheitskatalogs sind.

Als Kritische Infrastrukturen (KRITIS) sind Institutionen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen. Ohne funktionierende Informations- und Kommunikationstechnik kann keine Bank arbeiten, der Verkehr nicht fließen und die Industrie nicht produzieren. Und ohne Strom kommt die Gesellschaft erst recht zum Erliegen. Nahezu jeder Bereich unseres täglichen Lebens wird durch Informations- und Kommunikationstechnologie (IKT) unterstützt. Die Versorgung mit Energie spielt hier eine so wesentliche Rolle, dass der Gesetzgeber den Anbietern kritischer Infrastrukturen strenge Vorgaben macht. Dies gilt besonders für die Frage, wie Energieversorger ihre IT-Systeme zur unmittelbaren Netzsteuerung absichern.

Bis zum 31.01.2018 bleibt ihnen Zeit, um ein Informationsmanagementsystem nach ISO 27001 aufzusetzen (Abb.1: mdex ISO 27001 ISMS) und sich nach diesem zertifizieren zu lassen.

Ob die geringe Zahl der Zertifizierer, die bis heute existiert, dafür ausreicht, alle Unternehmen innerhalb dieses Zeitfensters zu zertifizieren, muss sich erst noch zeigen. In jedem Fall aber bringt der Zertifizierungsprozess für jedes Unternehmen, das ihn durchläuft, erheblichen Aufwand mit sich. Erfahrungen bei IT-Unternehmen haben gezeigt, dass mit einem Aufwand von mindestens 6 bis 12 Monaten auszugehen ist. Bei den Energieversorgern ist mindestens mit einem vergleichbaren Zeitramen zu rechnen.

Abbildung 2: ISO 27001-Siegel

mdexExperts - Zertifizierte Sicherheit als Service

IT-Sicherheitsanforderungen gemäß ISO 27001

Zertifizierte Komponenten müssen nicht erneut zertifiziert werden

Viele Sicherheitsverantwortliche bei den Versorgern stehen nun vor der Herausforderung, die Vorgaben rechtzeitig und mit vertretbarem Ressourcenaufwand zu erfüllen. Angesichts der heterogenen, gewachsenen IT-Landschaften bei vielen Stadtwerken ist dies keine einfache Aufgabe. Diese IT-Infrastrukturen bestehen häufig aus vielen unterschiedlichen Komponenten von einer Vielzahl verschiedener Hersteller. Als sie konzipiert wurden, standen andere Themen statt der heute geforderten, hohen Anforderungen an die IT-Sicherheit, im Fokus. Die Stabilität, die Flexibilität oder die hohe Verfügbarkeit einer Lösung hatte einen höheren Stellenwert als beispielsweise eine durchgehende Verschlüsselung des Datenverkehrs.

Abbildung 3: mdex Managed Service

Das größte Potenzial den hohen Anforderungen beim Thema Zertifizierung strategisch zu begegnen, bietet das so genannte Scoping (Festlegung des Geltungsbereichs der Zertifizierung). Dabei geht es darum, die Komplexität der Zertifizierung zu reduzieren. Eine Alternative zur Zertifizierung des Unternehmens insgesamt kann es beispielsweise sein, nur die Teile der IT zertifizieren zu lassen, die wirklich zertifiziert werden müssen. Zu diesen gehört jede IT-Komponente, die der unmittelbaren Netzsteuerung dient, nicht aber beispielsweise die Bürokommunikation.

Neben der Strategie, nur die betroffenen Teile zu zertifizieren, gibt es auch die Möglichkeit, Teile der Infrastruktur auszulagern. Die Steuerung des Netzes und der Betrieb der Leitstellen müssen intern und in Eigenregie durchgeführt werden. Dagegen kann zum Beispiel die Geräteanbindung nach Außen auch im Rahmen eines nach ISO 27001 zertifizierten Informationsmanagementsystems an einen geeigneten Dienstleister ausgelagert werden.

Eine Strategie, um die Anforderungen des IT-Sicherheitsgesetzes zu erfüllen, könnte also auf der einen Seite der Fokus auf die eigene Kernkompetenz sein, beispielsweise beim Thema Leitstelle. Und auf der anderen Seite könnte das Auslagern von Komponenten außerhalb des Kerngeschäftes - zum Beispiel bei der Anlagenanbindung - im Zusammenspiel mit der Nutzung von bereits zertifizierten Systembausteinen den Rücken für das Kerngeschäft freihalten.

Die Zertifizierung wird ab Werk mitgeliefert

Das Problem, die der Netzsteuerung dienenden Komponenten ISO 27001 konform zu betreiben, kann durch einen Appliance, bestehend aus einem Stück zertifizierter Dienstleistung und darauf abgestimmter Soft- und Hardware, gelöst werden.

Alle angebundenen Geräte kommunizieren miteinander dabei über ein so genanntes virtuelles privates Netzwerk (VPN) und bilden eine geschlossene Benutzergruppe. Die Appliance verwaltet alle eingehenden und ausgehenden Datenverbindungen. Mit Hilfe der VPN-Technologie werden Daten durchgehend verschlüsselt übertragen, sodass Unbefugte sie nicht mitlesen oder manipulieren können. Ein Energieversorger kann auf diese Weise alle Arten von Endgeräten mit der Leitstelle vernetzen. Die Appliance ist dabei die zentrale Komponente, über die die einzelnen Bestandteile solch eines Netzes integriert werden. Um hier einen „Single Point Of Failure“ zu vermeiden, sollte diese natürlich redundant aufgebaut sein.

Um auch „wildgewachsene“ Systemlandschaften sicher vernetzen zu können, gibt es unterschiedliche Verfahren zur Anbindung. Geräte und Leitungen lassen sich über DSL-Kabel, Mobilfunk und sogar über Satellit verbinden. Wichtig ist dabei nur, dass die Komponenten zur Anbindung IP-basiert arbeiten, über welche dann die VPN-Verbindung aufgebaut wird. Dies ist ein Ansatz, der optimal auf die Anforderungen von Energieversorgern abgestimmt ist, deren Systemlandschaften historisch gewachsen sind. Messstationen, EEG Anlagen, Ortsnetzstationen, Überwachungsanlagen

oder andere Teile des Netzwerks, die in Gebieten ohne Mobilfunkabdeckung stehen, können ebenso sicher an eine Leitstelle angekoppelt werden wie ein Computer, der auf einem Tisch neben dem zentralen Server steht und per Netzwerkkabel mit ihm verbunden ist. Auch redundante, ausfallsichere Netze lassen sich auf dieser Grundlage aufbauen. Das gilt selbst dann, wenn völlig unterschiedliche Hardware-Komponenten und Geräte zusammen genutzt werden. Das verwendete VPN-Protokoll sollte dabei ein offener Standard, wie z.B. IPsec oder OpenVPN, sein.

Eigenes Know-how ist nicht erforderlich

Unternehmen müssen nur wenige Voraussetzungen erfüllen, um Netzbausteine als zertifizierte Komponenten zu nutzen. Dazu gehört etwa, dass die notwendigen Server in einem abschließbaren Raum betrieben werden, der mit einer Alarmanlage gesichert ist. Größere Vorkenntnisse oder eine große IT-Abteilung sind darüber hinaus aber nicht notwendig, um mit Hilfe der Appliance sichere Netze zu knüpfen. Im Zuge eines Managed Service können spezialisierte Dienstleister die Arbeit übernehmen (Abb. 2: mdex Managed Service).

Üblicherweise umfasst das Aufstellen der Appliance gemäß der Zertifizierungsvorgabe in einem abgeschlossenen, alarmgesicherten Raum, den Anschluss, die dauerhafte Betreuung des Netzwerkes sowie die fortlaufende Aktualisierung der eingesetzten Software.

Die Aktualisierung sollte zudem durch Service-Verträge fortlaufend gesichert werden, sodass die Vernetzungslösung nicht veraltet. So sollten beispielsweise regelmäßig Updates zur Verfügung gestellt werden, die Schwachstellen in den Softwarebausteinen schließen. Damit ist die Investitionssicherheit einer solchen Lösung gewährleistet, und die durchgängig auf zertifizierten Bestandteilen aufgebaute Technologie ist hinreichend flexibel, um sich an neue Gegebenheiten anzupassen.

Zugleich bleiben die Energieversorger immer „Herr im eigenen Haus“. Während Servicedienstleister sich um den Betrieb und die technische Pflege des Netzwerks kümmern, bleiben Server, Netz und natürlich auch die Daten weiter in der Hand des Auftraggebers. Das gilt auch nach Ende eines Servicevertrages.

Die fortlaufende Pflege eines wild gewachsenen Netzwerkes beansprucht bislang enorme Ressourcen. Denn Sicherheitsupdates per Datenträger oder Einzeldownload in ein Netzwerk mit vielen unterschiedlichen Komponenten auszurollen ist in der Praxis für die IT-Organisation eines Stadtwerks oder eines vergleichbaren Anbieters kaum zu leisten.

In der Praxis wird deshalb mitunter an einigen Stellen einfach ganz auf eine Aktualisierung der Komponenten verzichtet. Das ist aus Sicherheitssicht natürlich nicht empfehlenswert.

Um Updates auch in weit verteilten Netzen auszurollen, ist in der Regel „FOTA“ das Mittel der Wahl. Das Kürzel FOTA steht für Firmware-Over-the-Air – Software-Aktualisierungen der Firmware, die über die Luftschnittstelle, beziehungsweise remote eingespielt werden. Diese Updates sollten natürlich nur in Absprache mit dem Kunden ausgerollt werden.

Die Vorteile: Weil die Software-Komponenten der Appliance ständig aktualisiert und weiterentwickelt werden, veralten sie nicht. Auch in fünf oder zehn Jahren sind sie auf dem neuesten Stand, während es heute Realität ist, dass in vielen Bereichen der Energiewirtschaft Geräte im Einsatz sind, bei denen die Software veraltet und dementsprechend unsicher ist. Und im Gegensatz zu dem großen Aufwand, der bislang bei der Modernisierung oder beim Ausrollen von Sicherheits-Updates anfiel, verursacht nun die Versorgung mit neuem Code keinen großen Aufwand.

Abbildung 4: mdex Security Rack

In der Summe bedeutet das, dass die Erzeuger sich trotz der anspruchsvollen ISO 27001-Vorgaben zur Sicherheit von IT-Systemen durch derartige Service-Angebote weiter voll auf ihr Kerngeschäft konzentrieren können. Die Zertifizierung wird vereinfacht, die Komplexität des eigenen Netzwerks reduziert, die Lösung veraltet nicht und für den Betrieb sorgt der Servicepartner. Und trotz aller Serviceleistungen behält der Versorger Daten und Leitungen in der eignen Hand. Mit dem Unterschied, dass das Netzwerk jetzt so sicher ist und hier das Thema Zertifizierung keinen Kopfschmerz mehr bereitet.

Als ISO 27001 zertifizierter IKT-Diestleister bietet mdex eine solche Appliance unter dem Namen „mdex Security Rack“ an (Abb. 4: mdex Security Rack).

mdexExperts - Zertifizierte Sicherheit als Service

IT-Sicherheitsanforderungen gemäß ISO 27001

IKT-Sicherheit mit mdex

Als ISO/IEC 27001 zertifizierter IKT-Dienstleister für die Energiebranche hat mdex bereits weitreichende Erfahrungen mit ISO/IEC-27001-konformen Kommunikationslösungen gesammelt, zum Beispiel bei der Steuerung und Überwachung von Ortsnetzstationen, dem EEG-Einspeisemanagement oder im anspruchsvollen Regelenergiemarkt.

Die datentechnische Anbindung der Energieanlagen kann über unterschiedliche Transportmedien wie DSL, Mobilfunk oder Satellit erfolgen. Sie fügt sich schnell und einfach in die bereits vorhandene IKT-Infrastruktur ein - ein „ISO 27001 Plugin“ gewissermaßen. Dabei werden alle benötigten Kommunikationselemente einschaltfertig aus einer Hand geliefert und während ihres gesamten Lebenszyklus gemanaged - inklusive Konfigurations- und Firmware-Updates.

Der Betrieb der zertifizierten IKT-Infrastruktur ist auch direkt beim Kunden möglich.

Sie haben Fragen zum Thema IKT-Sicherheit? Wir beraten Sie gerne.

Telefon: 04109 555 444 | **Email:** frage@mdex.de

www.mdex.de