Fragen und Antworten zur Zertifizierung nach IT-Sicherheitskatalog

Unsere Experten beantworten Ihnen hier die wichtigsten Fragen zur Zertifizierung nach IT-Sicherheitskatalog. Sie möchten noch mehr über die Zertifizierung wissen? **Kontaktieren Sie uns!**

1. WAS IST DER IT-SICHERHEITSKATALOG?

Der IT-Sicherheitskatalog wurde im August 2015 von der Bundesnetzagentur (BNetzA) auf der Grundlage von § 11 Abs. 1a des Energiewirtschaftsgesetzes (EnWG) veröffentlicht. Er fordert unter anderem als Mindeststandard die Einführung und Umsetzung eines Informationssicherheits-Managementsystems (ISMS) gemäß der DIN ISO/IEC 27001. Mit Ihrer Zertifizierung nach dem IT-Sicherheitskatalog gewährleisten Sie als Strom- oder Gasnetzbetreiber, dass Sie angemessene Schutzmaßnahmen gegen Bedrohungen für Telekommunikations- und elektronischen Datenverarbeitungssysteme umsetzen. Nicht nur zu dem Schutz Ihrer eigenen Technologie, auch zur Sicherstellung der Energieversorgung der Bevölkerung.

2. BIN ICH VERPFLICHTET DIE VORGABEN DES IT-SICHERHEITSKATALOGS UMZUSETZEN?

Ja, als Betreiber eines Strom- und Gasnetzes sind Sie zur Umsetzung des IT-Sicherheitskatalogs verpflichtet.

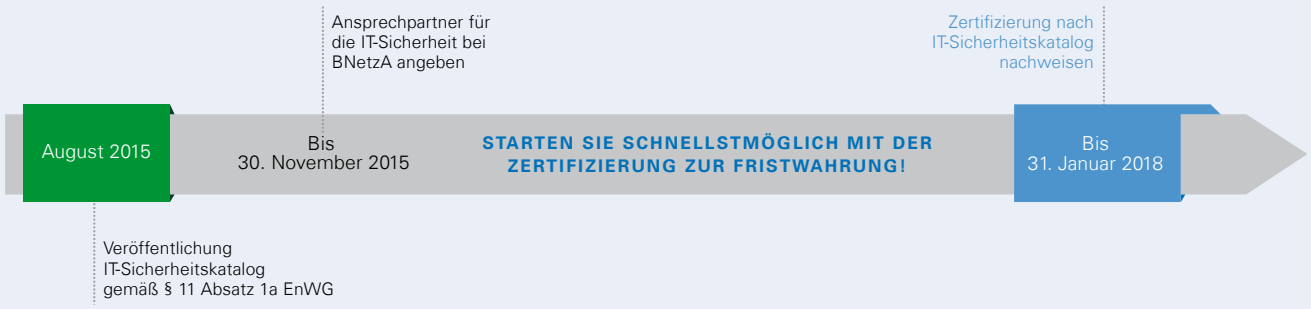
www.tuv.com/it-sicherheitskatalog

TÜVRheinland®
Genau. Richtig.

3. GIBT ES VERBINDLICHE FRISTEN?

Ja, bis spätestens 31. Januar 2018 müssen Sie nachweisen können, dass Sie die Vorgaben des IT-Sicherheitskatalogs für den „sicheren Netzbetrieb“ umgesetzt haben. Diesen Nachweis müssen Sie in Form einer Kopie Ihrer Zertifizierung an die Bundesnetzagentur senden.

ZERTIFIZIERUNG NACH IT-SICHERHEITSKATALOG



Außerdem müssen Sie seit dem 30. November 2015 der Bundesnetzagentur einen Ansprechpartner benennen, der für die Kommunikation bei auftretenden Sicherheitsvorfällen zuständig ist.

Wir empfehlen Ihnen umgehend mit der Bestandsaufnahme zu beginnen, um die IT-Sicherheitskatalog-Zertifizierung innerhalb der Fristen sicherzustellen!

Wir stehen Ihnen als kompetenter Zertifizierungspartner zur Seite. Sprechen Sie uns gerne an!

4. WIE IST DER ABLAUF EINER ZERTIFIZIERUNG?

Der Zertifizierungsablauf zum IT-Sicherheitskatalog setzt sich aus sechs Schritten zusammen:

1. **Bestandsaufnahme (optional)**
   Erfassung des Ist-Zustands und Untersuchung, welche Anforderungen bereits erfüllt werden. Wir empfehlen, diese durchführen zu lassen.
2. **Zertifizierungsaudit Stufe 1 (Dokumentenprüfung)**
   Unterstützende Prüfung der Umsetzung der festgelegten Ziele und Anforderungen
3. **Zertifizierungsaudit Stufe 2 (Prüfung der Umsetzung)**
   Prüfung der Umsetzung der festgelegten Schutzziele und der Vorgaben des IT-Sicherheitskatalogs.
4. **Zertifikatserteilung**
   Nach erfolgreichem Zertifizierungsverfahren erhalten Sie Ihr Zertifikat
5. **Jährliche Überwachungsaudits**
   Unterstützung bei der kontinuierlichen Optimierung Ihrer Prozesse
6. **Re-Zertifizierung**
   Vor Ablauf von drei Jahren findet eine Re-Zertifizierung statt

www.tuv.com/it-sicherheitskatalog

5. WELCHE VORTEILE BIETET MIR EINE ZERTIFIZIERUNG NACH DEM IT-SICHERHEITSKATALOG?

Sie erfüllen mit der Zertifizierung nach IT-Sicherheitskatalog nicht nur die Vorgaben der Bundesnetzagentur sondern schließen auch gewisse Haftungsrisiken aus, optimieren die Unternehmensprozesse und steigern die Produktivität.

Vorteile einer IT-Sicherheitszertifizierung

Erfüllung der Anforderungen des IT-Sicherheitskatalogs gem. § 11 Abs. 1a EnWG

Erhalt eines gesetzlich vorgeschriebenen Zertifikats

Sicherstellung Ihrer zu schützenden Systeme und Daten

Prozessverbesserung und Produktivitätssteigerung

Reduzierung der Haftungsrisiken

Wettbewerbsvorteil

Imagesteigerung in der Öffentlichkeit und bei Geschäftspartnern

Erfüllung der Kundenerwartungen

6. MUSS ICH AUCH TEILE MEINES SYSTEMS ZERTIFIZIEREN LASSEN, DIE DURCH EXTERNE DRITTE BETRIEBEN WERDEN?

Ja, auch wenn die vom IT-Sicherheitskatalog betroffenen Anwendungen, Systeme und Komponenten durch Dritte (Outsourcing, externe Dienstleister) betrieben werden, sind Sie nicht von Ihrer Verantwortung entbunden. Sie müssen mit dem Dienstleister durch vertragliche Vereinbarungen festlegen, dass er sich an die vorgeschriebenen Sicherheitsanforderungen des IT-Sicherheitskatalogs hält. Ausgenommen ist der Fall, dass die Anlagen ohne Gefährdungspotential, ohne Anschluss an das Leitsystem oder in das Internet betrieben werden. Können Sie dies mit einem begründeten Nachweis belegen, besteht keine Umsetzungspflicht für die diesbezüglichen Sicherheitsanforderungen.

7. WELCHE BEREICHE UMFASST DER IT-SICHERHEITSKATALOG?

Der Geltungsbereich (Scope) umfasst alle Anwendungen, Systeme und Komponenten, die für den sicheren Netzwerkbetrieb nötig sind. Enthalten sind IT- und Telekommunikations-Systeme, die bei einem Ausfall direkt oder indirekt Ihre Netzwerksicherheit gefährden. Jede Zertifizierung weist auf, für welchen Geltungsbereich die Einhaltung der Norm bewertet und geprüft wurde.

8. IST MEINE ZERTIFIZIERUNG NACH DIN ISO 27001 ODER BSI GRUNDSCHUTZ BEREITS AUSREICHEND?

Nein, diese Zertifizierungen alleine reichen nicht aus, um alle nötigen Anforderungen des IT-Sicherheitskatalogs abzudecken.

9. WIE SETZT SICH DIE ZERTIFIZIERUNG NACH IT-SICHERHEITSKATALOG ZUSAMMEN?

- Es muss ein „Informationssicherheits-Managementsystem“ gemäß ISO/IEC 27001 implementiert werden.
- Es sind „Sicherheitskategorien und Maßnahmen“ gemäß der im Anhang „A“ der ISO/IEC 27001 (ISO/IEC 27002) erweitert um die ISO/IEC TR 27019 umzusetzen.
- Der nachhaltige „Ordnungsgemäße Betrieb der betroffenen IKT-Systeme“ ist von den Netzbetreibern sicherzustellen.
- Der Netzbetreiber hat einen „Netzstrukturplan“ anzufertigen und zu pflegen. Dieser muss mindestens die Technologiekategorien „Leitsystem und Systembetrieb“, „Übertragungstechnik/Kommunikation“ und „Sekundär-, Automatisierungs- und Fernwirktechnik“ umfassen, welche im Geltungsbereich liegen.
- Es muss ein „Prozess zur Risikoeinschätzung“ gemäß Kapital 6,1,2 der ISO/IEC 27001:2015-3 existieren.
- Es muss ein „Prozess zur Risikobehandlung“ gemäß Kapital 6,1,2 der ISO/IEC 27001:2015-3 existieren.
- Es muss ein „Ansprechpartner IT-Sicherheit“ bestellt und an die BNetzA gemeldet worden sein.

10. WELCHE ZIELE HAT DER IT-SICHERHEITSKATALOG?

Die Inhalte des IT-Sicherheitskatalogs zielen darauf ab, einen sicheren Netzbetrieb zu gewährleisten, indem Telekommunikations- (TK) und elektronische Datenverarbeitungssysteme (EDV) vor Bedrohungen geschützt werden, welche unverzichtbar für den sicheren Netzbetrieb sind. Folgende Ziele sollen dabei erreicht werden:

- Sicherstellung der Verfügbarkeit der zu schützenden Systeme und Daten
- Sicherung der IT- und Kommunikationstechnik, die den Netzbetrieb sicherstellen
- Sicherstellung der Integrität der verarbeiteten Informationen und Systeme
- Gewährleistung der Vertraulichkeit der mit den betrachteten Systemen verarbeiteten Informationen

SIE HABEN WEITERE FRAGEN? UNSERE EXPERTEN STEHEN IHNEN MIT EINEM KOSTENFREIEN INFORMATIONSGESPRÄCH ZUR VERFÜGUNG. SPRECHEN SIE UNS HIERZU GERNE AN!

ONLINE KONTAKT

TÜV Rheinland Group
TÜV Rheinland Cert GmbH
Am Grauen Stein
51105 Köln
Tel. +49 800 888 2378
Fax. +49 800 888 3296
tuvcert@de.tuv.com
www.tuv.com/it-sicherheitskatalog

TÜVRheinland®
Genau. Richtig.