Datenblatt zum IT-Sicherheitsgesetz (ITSiG)

Mit dem IT-Sicherheitsgesetz wird die Einhaltung von Mindeststandards für die IT-Sicherheit verpflichtend.

Mit Inkrafttreten des IT-Sicherheitsgesetzes (ITSiG) werden Betreiber besonders gefährdeter Infrastrukturen (sogenannte „Kritische Infrastrukturen") aus Bereichen wie z.B. Energie, Informationstechnik, Telekommunikation, Gesundheit, Wasser oder Ernährung verpflichtet, ihre Systeme und Anlagen besser vor Cyber-Angriffen zu schützen. Neben der Meldung von IT-Sicherheitsvorfällen betsteht eine Verpflichtung, die Erfüllung der gesetzlichen Anforderungen alle zwei Jahre nachzuweisen!

Unser Ziel ist es diese Verpflichtungen und Anforderungen angepasst an die Unternehmensgröße und dem finanziellen Rahmen zu ermöglichen.

Die Einhaltung von IT-Sicherheitsmaßnahmen in der Produktion wird für die betroffenen Unternehmen verpflichtend sein. Dazu gehören z.B. aktuelle IT-Dokumentation, kontinuierliche Überwachung, Viren- und Internetschutz, Datensicherungen, Passwortmanagement, Umgang mit externen Dienstleistern, etc. Der Fokus liegt dabei auf pragmatischen und organisatorischen Schritten sowie auf technischen Lösungen. Die Anforderung besteht darin, die Wirksamkeit für die Unternehmen im Betriebsprozess zu etablieren.

Ziel ist es, die IT-Risiken in Produktionsanlagen zu minimieren und finanzielle Schäden in Problemsituationen im Griff zu haben. Die Abhängigkeit von der IT gestaltet sich damit kontrollierbar. Mehrfachaufwendungen wie z.B. die manuelle Aufnahme und Prüfung von IT-Systemen sollten aus wirtschaftlichen Gesichtspunkten vermieden werden.

Der Einführung des ITSiG können Unternehmen durch die Umsetzung der nun folgenden Maßnahmen ohne große Bedenken entgegensehen.

Anforderungen durch das ITSiG:

Anforderungen

an die Betreiber

- Benennung einer ständig erreichbaren Kontaktperson für das Bundesamt für Sicherheit in der Informationstechnik (BSI), Kontaktpersonen können auch mit mehreren Unternehmen gemeinsam eingerichtet werden (§ 8b Abs. 3 BSIG)
- Verpflichtung zur Meldung von IT-Störungen an das BSI, zur Warnung weiterer potentiell Gefährdeter
- Erstellung eines Lageberichts über die IT-Sicherheit in Deutschland zu unterstützen (§ 8b Abs. 4f. BSIG)
- „Anonyme Meldung“ nur bei Gefährdung von Systemen, nicht bei Eintritt einer Störung
- Pflichten bestehen auch dann, wenn Unternehmen ihre IT durch Dienstleister betreiben lassen!

Maßnahmen

zur Erfassung

- der informationstechnischen Systeme
- der informationstechnischen Komponenten
- der Vorgänge der Informationsverarbeitung

Die Absicherungsmaßnahmen müssen an Stellen eingehalten werden, an denen die Informationstechnik Einfluss auf die Erbringung von Dienstleistungen hat. Organisatorische und technische Vorkehrungen zur Abschottung besonders kritischer Prozesse, inkl. infrastruktureller und personeller Maßnahmen, gilt es zu berücksichtigen.

Bestimmungen

zum Stand der Technik

- Einschlägige internationale, europäische und nationale Normen und Standards oder vergleichbar effektiver Schutz
- Dokumentation in entsprechenden Sicherheits- und Notfallkonzepten
- Erarbeitung branchenspezifischer Sicherheitsstandards (hier DWA)

Dem einzelnen Betreiber steht es frei, auch eigene, dem Stand der Technik entsprechende, Maßnahmen umzusetzen. Die Maßnahmen müssen angemessen sein.

Nachweise

durch Sicherheitsaudits, Prüfungen oder Zertifizierungen:

- Information Security Management (Sicherheitsorganisation, IT-Risikomanagement etc.)
- Kritische Cyber-Assets werden identifiziert und gemanagt
- Maßnahmen zur Angriffsprävention und -erkennung
- Implementierung eines Business Continuity Managements (BCM)
- Branchenspezifische Besonderheiten

Auszug zu Maßnahmen für die Sicherheit in der Informationstechnik kritischer Infrastrukturen

Nr.	Maßnahme	**Erfüllt?**	Selbst	Admin	IRMA
IT-Sicherheits-Management (organisatorisch, personell)					
1.1	Ist ein IT-Sicherheitsverantwortlicher für die Produktionsanlagen von der Geschäftsleitung benannt?		■		
1.2.	Gibt es eine Sicherheitsleitlinie für die Produktionsanlagen (Bedeutung im Unternehmen, Sicherheitsziele)?		■		
	Sind alle relevanten Mitarbeiter zum Thema IT-Sicherheit sensibilisiert?		■		
	Kennen Sie Ihre kritischen, gegen Cyberangriffe zu schützenden Unternehmenswerte in der Produktion (Assets) und ist diese Erfassung aktuell?				■
	Sind die Risiken / Schutzbedarfe für diese Assets bekannt und bewertet?				■
IT-Sicherheitsmaßnahmen zur Angriffsprävention (technisch, infrastrukturell)					
2.1	Ist das Firmengelände gegen unberechtigten Zutritt geschützt?		■		
2.2	Ist der Zutritt zu IT-Systemräumen und anderen Räumen mit kritischen Systemen geregelt? (u.a. Besucherregelung)		■	■	
	Gibt es eine / mehrere Firewalls? Wird diese aktuell gehalten? Konfiguration? Changemanagement?			■	■
	Gibt es ein Konzept, wie der Fernzugriff von außen erfolgen muss? Sind Fernwartungszugänge entsprechend abgesichert?			■	■
	Sind alle unnötigen Dienste und Programmfunktionen deaktiviert?			■	■
	Existiert ein geregelter Ablauf für das Patchmanagement?			■	■
	Sind Web-Browser und E-Mail-Programm sicher konfiguriert? Ist aus dem Produktionsnetz heraus ein freier oder unbeschränkter Internetzugriff möglich?			■	■
	Werden flächendeckend Viren-Schutzprogramme eingesetzt? Sind diese aktuell?		■	■	
	Existiert ein Sicherheitskonzept für die Vernetzung der IT-Systeme mit mobilen Endgeräten? Ist externe Hardware (Smartphones, Laptops, USB,) im erlaubt?		■		■
	Befinden sich IT-Systeme mit demselben Schutzbedarf in eigenen Netzsegmenten?			■	■
	Ist geregelt, auf welche Datenbestände Mitarbeiter und Dienstleister zugreifen dürfen? Sind Zugriffe auf das Produktionsnetz von anderen Nutzern möglich?		■		
	Wie werden diese Maßnahmen kontrolliert? Kontinuierlich?		■	■	■
IT-Sicherheitsmaßnahmen zur Angriffserkennung					
	Erfolgt eine Erkennung von Cyberangriffen? Wird das IT-Netz der Produktion kontinuierlich auf Angriffe überwacht?				■
	Werden Systemdateien, Anwendungen, Konfigurationsdateien und Anwendungsparameter auf Integrität überprüft?			■	
	Ist die Nutzung (Logging) der Systeme nachvollziehbar?				■
Notfallvorsorge (BCM)					
	Gibt es einen Notfallplan mit Anweisungen und Kontaktadressen?		■		
	Werden Datensicherungen für alle unternehmenskritischen IT-Systeme durchgeführt?		■		
	Werden die Datensicherungen und das Rücksicherungsverfahren regelmäßig kontrolliert?		■		
Dokumentation					
	Sind die Systeme, Geräte und Zustand aktuell dokumentiert?				■
	Sind die Sicherheits- und Notfallkonzepte dokumentiert?		■		
	Existieren Verträge mit allen Dienstleistern mit Regelungen zur Systemverfügbarkeit und Vertraulichkeit?		■		

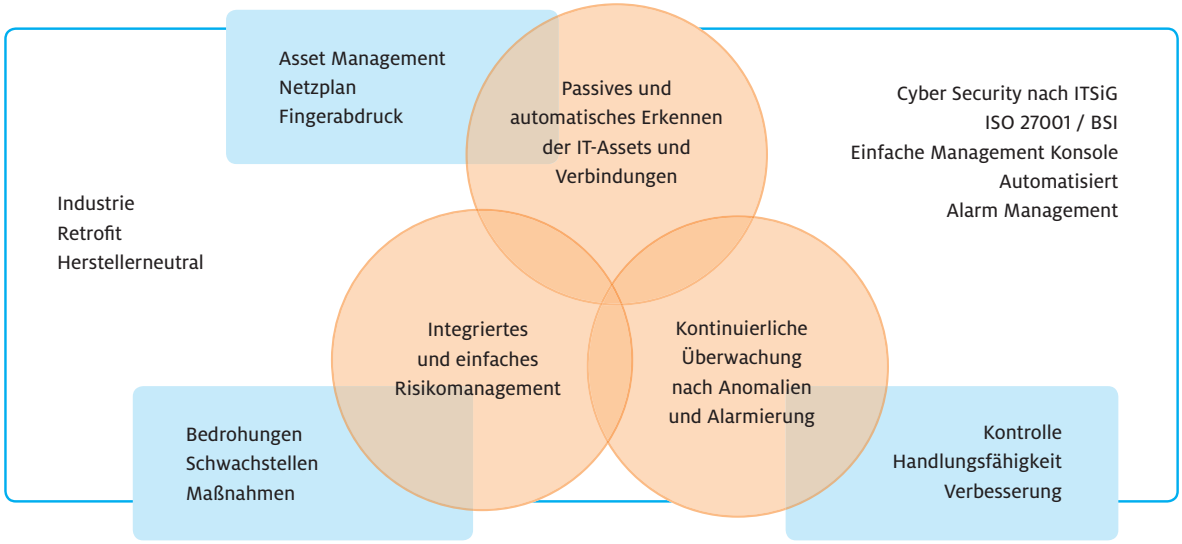
■ Schneller Erfolg! Erstmaßnahmen!

■ Eigene Maßnahmen können von der Betriebsleitung und Betriebsteam umgesetzt werden

■ Administration / Anpassung der vorhanden Komponenten (System, Geräte, Netzwerk, ...)

■ Effiziente Ergänzung zur schnellen Verbesserung der Cyber Sicherheit und Erfüllung des ITSiG.

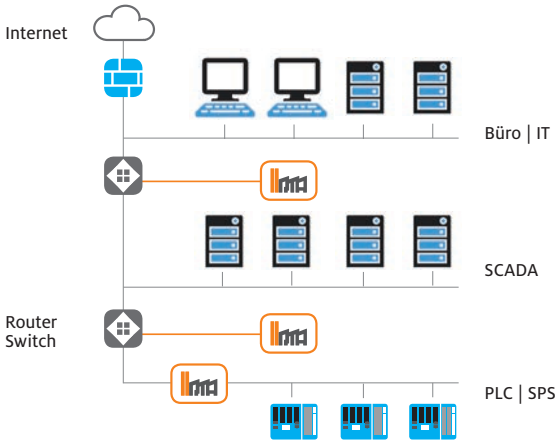
Industrie Risiko Management Automatisierung



Weitere Erfolgsfaktoren zur Umsetzung

- Passives scannen und Analyse der Teilnehmer und Verbindungen
- Validierung jeder Verbindung / jedes Teilnehmers
- Informationen für die Netzsegmentierung und Trennung mit Firewalls
- Kontinuierliche Überwachung der Anlagen und intelligente Alarmierungen
- Risiko Management inkl. Reporting nach ISO 27000 / BSI über den Zustand der gesamten Anlage

IRMA ist ein Industrie Computer System mit einer übersichtlichen Managementkonsole. Ohne jegliche Aktivitäten im Netzwerk der Produktionsanlage erfasst und analysiert IRMA die Systeme und Verbindungen. Durch die kontinuierliche Überwachung, Analyse und die intelligente Alarmierung bietet IRMA in Echtzeit Informationen zu Mißkonfigurationen oder Cyberangriffen. Das integrierte Risiko-Management ermöglicht es, umgehend über die maßgeblichen Aktionen zu entscheiden, um einen Angriff zu stoppen oder die Auswirkung zu entschärfen.



VIDEC GmbH
Contrescarpe 1 · DE-28203 Bremen · Phone +49(0)421 - 33 950-0 · Fax +49(0)421 - 33 950-50
info@videc.de · www.videc.de
Niederlassungen und internationale Vertretungen entnehmen Sie bitte unserer Website.

design: www.blaukontor.de

IRMA ist ein Produkt der ACHTWERK GmbH & Co KG. Alle Rechte vorbehalten.