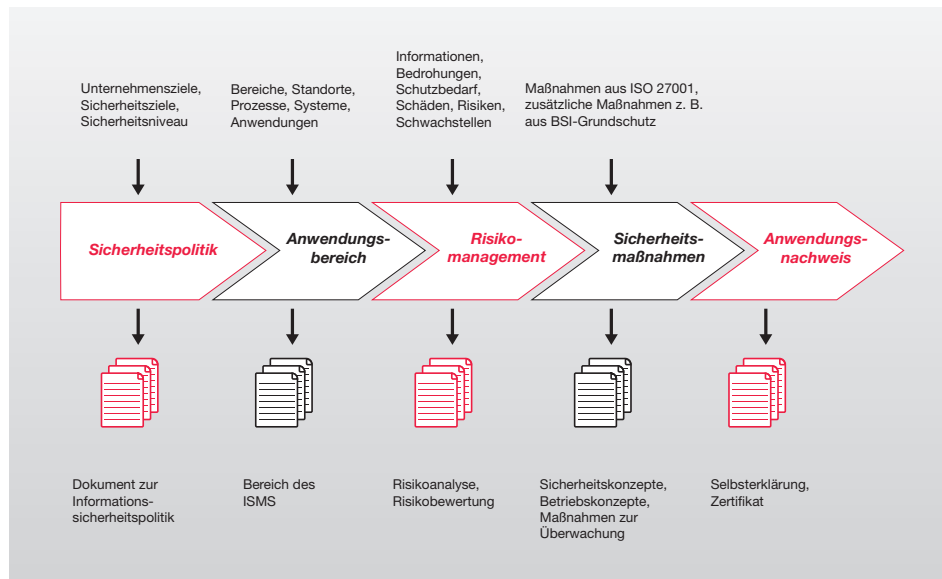


Ganzheitliche Sicherheitskonzepte nach ISO 27001



Ihre Vorteile:

- » **Umfassende Sicherheit durch ganzheitliches Konzept**
- » **Zielgerichtete Maßnahmen durch Expertenwissen**
- » **Hervorragendes Kosten-Nutzen-Verhältnis**

Informationen sind eine kritische Ressource in Unternehmen. Ihr Schutz vor unbefugter Kenntnisnahme, Veränderung oder Verlust ist wichtiger denn je. Sicherheitsmaßnahmen eines Unternehmens können ihre Wirkung nur dann entfalten, wenn sie in ein Gesamtkonzept der Informationssicherheit eingebunden sind. Gleichzeitig wird somit sichergestellt, dass gesetzliche Anforderungen, wie zum Beispiel an den Datenschutz oder das betriebliche Risikomanagement, erfüllt werden. **secunet hat umfangreiche Erfahrungen im Aufbau von ganzheitlichen Informationssicherheitsmanagementsystemen nach ISO 27001.** Wir beraten Sie unter Berücksichtigung Ihrer individuellen Anforderungen und Besonderheiten.

Kennen Sie Ihren Bedarf?

Für eine unternehmensspezifische Sicherheitsstrategie ist es in erster Linie wichtig, die eigenen Bedarfe zu erkennen. Welche Anforderungen an die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen gibt es? Wie lassen sich die im Unternehmen vorliegenden Informationen nach ihrer Sensibilität klassifizieren? Welche Prozesse und IT-Systeme sind kritisch für die Geschäftstätigkeit? Welche IT-Sicherheitsmaßnahmen sind bereits umgesetzt? Wo stehen Sie im Vergleich zur Best Practice bei anderen Unternehmen?

Basierend auf einer Analyse der Ist-Situation definieren wir mit Ihnen Sicherheitsanforderungen und formulieren Ihre IT-Sicherheitsstrategie.

Unternehmensweite Standards festlegen

Wenn versucht wird, IT-Sicherheit durch punktuelle Maßnahmen zu erreichen, entsteht häufig eine Ansammlung von unterschiedlichen, ggf. redundanten Sicherheitsmechanismen. Das ist nicht nur ineffizient, sondern führt auch zu Sicherheitsproblemen, weil grundlegende, unternehmensweit gültige Zusammenhänge in der Einzelbetrachtung nicht erkannt werden.

Deshalb empfiehlt es sich auf übergeordneter Ebene einheitliche Sicherheitsstandards zu definieren, die für Einzelprojekte verbindlich sind und ein durchgängiges Sicherheitsniveau gewährleisten. Eine international anerkannte Möglichkeit diesen Anforderungen gerecht zu werden, ist der Aufbau eines Informationssicherheitsmanagementsystems (ISMS), das nach der Norm ISO 27001 zertifiziert ist.

Risiken ermitteln

Damit IT-Sicherheit wirtschaftlich umgesetzt werden kann, müssen sich die Maßnahmen an den tatsächlich vorhandenen Risiken orientieren. Im Rahmen einer Risikoanalyse identifizieren unsere Experten mögliche Schadensszenarien und bewerten sie im Hinblick auf ihre Auswirkungen und die Wahrscheinlichkeit ihres Eintretens. Dabei setzen wir zur Bewertung erprobte Methodiken und Tools ein.

Maßnahmen definieren

Der Auswahl von Maßnahmen zur Erhöhung des IT-Sicherheitsniveaus kommt eine besondere Bedeutung zu. Sie müssen

- kosteneffizient und zukunftssicher sein,
- die übergeordnete Sicherheitsstrategie erfüllen,
- das Sicherheitsbewusstsein stärken und
- sich in den Unternehmenskontext einfügen.

Weitere Maßnahmenforderungen ergeben sich aus den Ansprüchen an eine moderne Arbeitsweise, wie zum Beispiel Mobilität, permanente Verfügbarkeit und Dynamik beim Datenaustausch. Für alle auftretenden Herausforderungen sind unseren Experten aktuelle Sicherheitslösungen und -produkte aus dem praktischen Einsatz vertraut.

Branchenspezifische Anforderungen erfüllen

Das IT-Sicherheitsmanagement muss nicht nur finanziellen Schäden begegnen. Auch die Einhaltung relevanter Gesetze und Regelungen (Compliance) bildet ein wichtiges Ziel, für das die Geschäftsleitung die persönliche Verantwortung trägt.

Dank unseres Branchenwissens können wir Ihnen aufzeigen, welche Anforderungen für Ihre Organisation relevant sind und wie Sie diese effizient erfüllen können. Unsere Sicherheitsdokumentation hilft Ihnen, die Einhaltung dieser Vorgaben gegenüber Dritten (z. B. Aufsichtsbehörden) nachzuweisen.

Sicherheit zertifizieren

Nachdem ein ISMS etabliert wurde, besteht die Möglichkeit, eine Zertifizierung nach der Norm ISO 27001 zu beantragen. Wir bieten Ihnen, bei Vorliegen aller Voraussetzungen, die Zertifizierung Ihres IT-Verbundes durch einen unserer ISO-27001-Auditoren an. Mit diesem international anerkannten Zertifikat können Sie ein funktionsfähiges ISMS belegen und verfügen damit über eines der wertvollsten, heute vorhandenen Sicherheitssiegel. So zeigen Sie, dass Sie dem Thema IT-Sicherheit einen hohen Stellenwert beimessen.

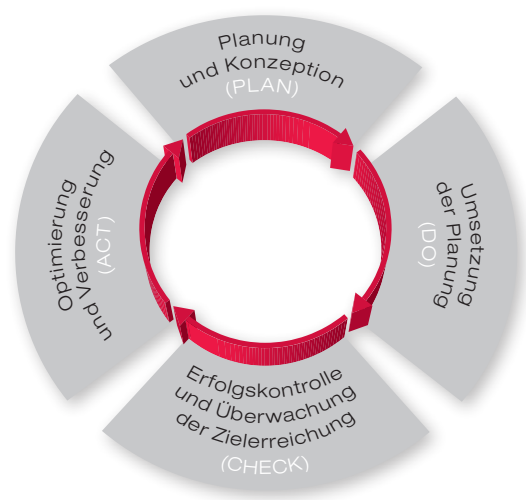
Wenn Sie sich nicht sicher sind, ob Sie alle Voraussetzungen für eine Zertifizierung erfüllen, bieten wir Ihnen darüber hinaus die Möglichkeit der Durchführung eines Vor-Audits. Der Ablauf ist vergleichbar mit einem Live-Audit, jedoch wird die Zertifizierungsstelle anschließend nicht direkt eingebunden.

Den Sicherheitsprozess in Gang bringen

Mit der Weiterentwicklung der Organisation und ihrer IT, aber auch durch äußere Einflüsse wie neue Angriffsmuster, technologische Fortentwicklung oder neue gesetzliche Anforderungen, müssen Sicherheitskonzepte beständig angepasst, erweitert und fortgeschrieben werden. Das funktioniert nur, wenn Sicherheit als ein Prozess fest im Unternehmen verankert und mit klaren Verantwortlichkeiten und Vorgehensmodellen unterlegt ist.

Wir unterstützen Sie dabei in jeder Phase dieses Prozesses:

- Auswahl und Abgrenzung des zu betrachtenden IT-Verbundes
- Schutzbedarfsfeststellung
- Risikoanalyse
- Maßnahmendefinition
- Umsetzung
- Zertifizierung



Unser oberstes Prinzip ist es, ein maßvolles und zweckoptimiertes Vorgehen zu implementieren, um über eine kontinuierliche Verbesserung der IT-Sicherheit das optimale Schutzniveau für Sie zu erreichen.

Weitere Informationen:
www.secunet.com/isms

secunet

secunet Security Networks AG
 Kronprinzenstraße 30
 45128 Essen

Tel.: +49-201-5454-0
 Fax: +49-201-5454-1000
 E-Mail: info@secunet.com
www.secunet.com