In 3 Schritten zur sicheren IT

VdS 10000
Der ganzheitliche Ansatz für Informationssicherheit

Mensch – Technik – Organisation

Schwachstellen in IT-Systemen sind beliebte Einfallstore für Schadsoftware und Hacker-angriffe. In den meisten Fällen werden Schwachstellen ausgenutzt, die oft allgemein bekannt sind und längst hätten geschlossen werden sollen.

Andererseits genügt es nicht, lediglich die Technik zu betrachten. Jeder Mensch macht Fehler und wenn Richtlinien zur Orientierung fehlen und falsch reagiert wird, können große Schäden entstehen. Ihre Informationssicherheit muss deshalb Mensch, Technik und Organisation in einem ganzheitlichen Ansatz berücksichtigen.

Gleichzeitig ist es wenig sinnvoll, wenn jedes Unternehmen versucht, das Rad neu zu erfinden. Verschiedene Standards zur Informationssicherheit stellen sicher, dass alle wichtigen Aspekte in einem Sicherheitskonzept angemessen berücksichtigt werden.

1. Sicherheitskonzept nach VdS 10000

Die VdS Richtlinie 10000 für die Informationssicherheit definiert Mindestanforderungen an ein Managementsystem für die Informationssicherheit für kleine und mittelständische Unternehmen. Sie basiert auf den anerkannten Standards ISO 27001 und BSI Grundschutz.

Mit ca. 20 % des Aufwands im Vergleich zu ISO 27001 kann Ihr Unternehmen aus den VdS-Richtlinien Maßnahmen und Prozesse ableiten, mit denen Sie in der Informationstechnik ein angemessenes Schutzniveau erreichen. Zusätzlich wurden die VdS-Richtlinien aufwärtskompatibel gestaltet. Dadurch kann eine Zertifizierung nach VdS 10000 auch jederzeit der Einstieg in ISO 27001 sein, bei dem wir Sie ebenfalls gerne unterstützten.

Was Sie von uns erwarten können

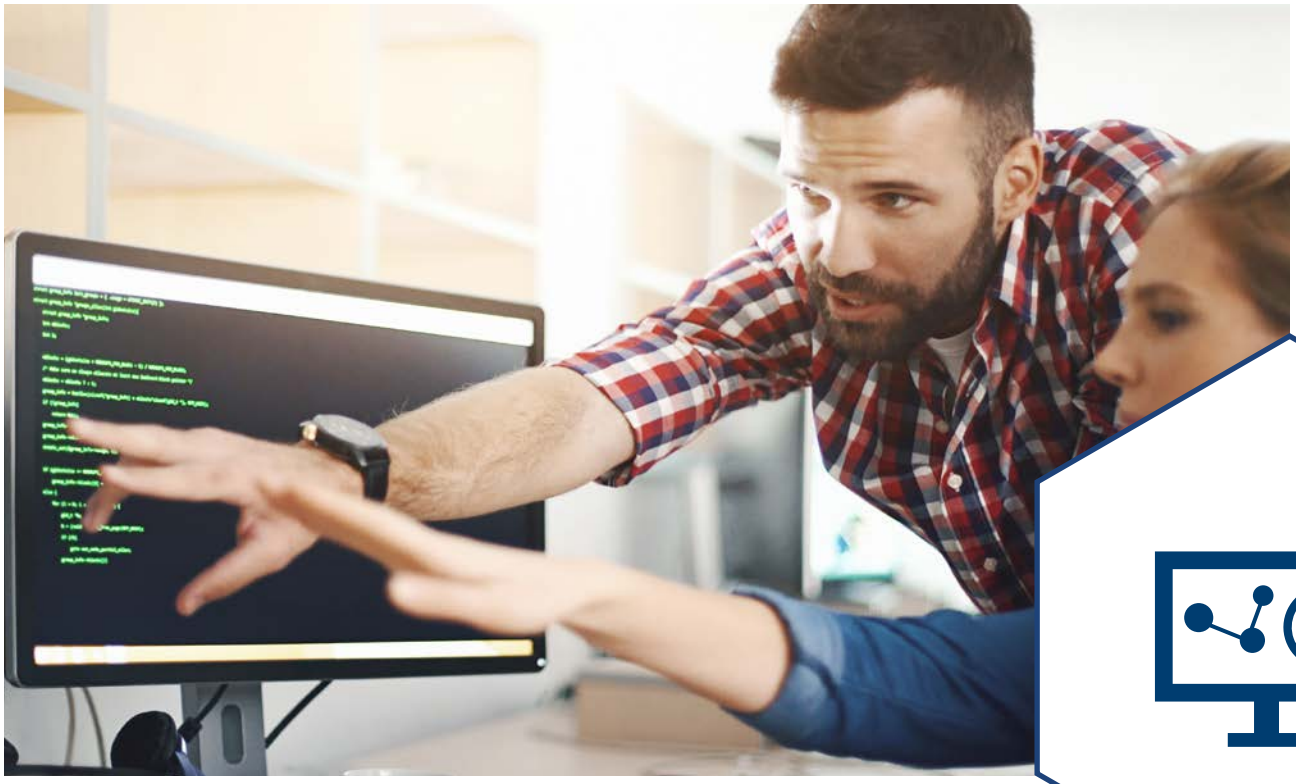
Wir liefern Ihnen Vorlagen zu allen notwendigen Richtlinien und Verfahren, die wir zusammen mit Ihnen an Ihre Bedürfnisse anpassen. Während der gesamten Erstellung stehen wir Ihnen beratend zur Seite und stellen sicher, dass die Anforderungen der VdS 10000 eingehalten werden. Darüber hinaus unterstützen wir Sie bei der Einführung der notwendigen Prozesse und führen anschließend ein internes Audit durch.

Außerdem bereiten wir Sie falls gewünscht auf die Zertifizierung durch das Auditorenteam der VdS vor.

2. Umsetzung der technischen Maßnahmen

Aus den im ersten Schritt entwickelten Sicherheitsrichtlinien und Verfahren ergibt sich in der Regel weiterer Handlungsbedarf.

Vielleicht müssen Server gehärtet, d.h. angepasst und sicherer konfiguriert werden. Gegebenenfalls müssen auch zusätzliche Lösungen wie Log-Management oder APT-Schutz integriert werden. Außerdem muss das Zusammenspiel zwischen eigenen und Cloud-basierten Systemen berücksichtigt werden.



Was Sie von uns erwarten können

Wir entwickeln zusammen mit Ihnen einen Plan zur Umsetzung und ergänzen diesen mit Dokumentationen und Empfehlungen sowie konkreten Details. Wir evaluieren bei Bedarf Produkte und wählen für Sie geeignete Lösungen aus.

Falls gewünscht setzen wir diese Maßnahmen auch für Sie um. Beispielsweise ergänzen wir die Gruppenrichtlinien Ihrer Windows-Domäne, optimieren Firewall-Regeln und verstärken Ihren VPN-Zugang durch Zweifaktorauthentisierung.

3. Sensibilisierung Ihrer Mitarbeiter

Informationssicherheit kann immer nur so gut sein, wie sie von Ihren Mitarbeitern akzeptiert und unterstützt wird. Schulungen und Workshops dienen der Sensibilisierung Ihrer Mitarbeiter.

Hier werden von uns einerseits die Richtlinien und Verfahren Ihres Sicherheitskonzepts In diesen Workshops werden von uns die Richtlinien und Verfahren Ihres Sicherheitskonzepts vorgestellt und ihre Notwendigkeit erläutert. Weiterhin werden Gefährdungen aufgezeigt und das richtige Verhalten z.B. beim Erhalt von Phishing-Mails oder bei Verdacht einer Schadcodeinfektion vermittelt.

Was Sie von uns erwarten können

Wir stellen Ihren Mitarbeitern Ihr Sicherheitskonzept vor und erläutern leicht verständlich die Hintergründe und den Nutzen. Mit anschaulichen Beispielen zeigen wir live wie Hackingangriffe ablaufen und Schadsoftware Systeme infiziert und erklären, wie diese Angriffe verhindert werden können. Insbesondere erklären wir, wie Ihre Mitarbeiter das Unternehmen dabei unterstützen können.

Im Falle einer geplanten VdS-Zertifizierung bereiten wir Ihre Mitarbeiter außerdem auf das Audit vor.

Ihre Vorteile

Mit einer zertifizierten Informationssicherheit nach VdS 10000 ergeben sich für Ihr Unternehmen eine Vielzahl von Vorteilen:

- Das VdS-Zertifikat bestätigt, dass sich Ihr Unternehmen organisatorisch, technisch und personell auf die wichtigsten Angriffsszenarien vorbereitet hat und über passende Prozesse und Schutzmaßnahmen verfügt.

- Das VdS-Zertifikat erzeugt bei Lieferanten, Kunden und Versicherern ein hohes Vertrauen in die Leistungsfähigkeit Ihres Unternehmens. Daten sind sicher geschützt und die Risiken zu Einschränkungen der Lieferfähigkeit Ihres Unternehmens wurden minimiert. Wettbewerbsvorteile sind die Folge.

Aber auch ohne Zertifizierung können Sie profitieren:

- Ihr Unternehmen gewinnt wertvolles Wissen zur Informationssicherheit, ein wichtiger Aspekt auch in der voranschreitenden Digitalisierung.

- Ihr Unternehmen erweitert sein Risikomanagement um den Aspekt der Informationssicherheit. Ein unabdingbares Muss für die Unternehmenssicherheit.

- Die Risikotransparenz im Unternehmen wird erhöht und so die Geschäftsleitung entlastet. Ihr Unternehmen kann sich verstärkt auf seine Kernprozesse konzentrieren.

- Das – immer verbleibende – Restrisiko kann Ihr Unternehmen leichter und günstiger auf einen Versicherer übertragen und damit eine weitere Verteidigungslinie für Ihre Existenzsicherung aufbauen.

DSGVO: VdS 10010

Übrigens, auch im Datenschutz und der Umsetzung der Anforderungen der Datenschutzgrundverordnung (DSGVO) können wir Sie unterstützen. Gerne auch in Zusammenarbeit mit Ihrem Datenschutzbeauftragten.

Mit dem kompakten und speziell auf kleine und mittelständische Unternehmen zugeschnittenen Leitfaden der VdS 10010 können Sie die rechtlichen, organisatorischen und technischen Anforderungen der DSGVO klar strukturiert und mit überschaubarem Aufwand umsetzen. Die Richtlinien VdS 10010 sind eng verzahnt mit der VdS 10000 zur Informationssicherheit.

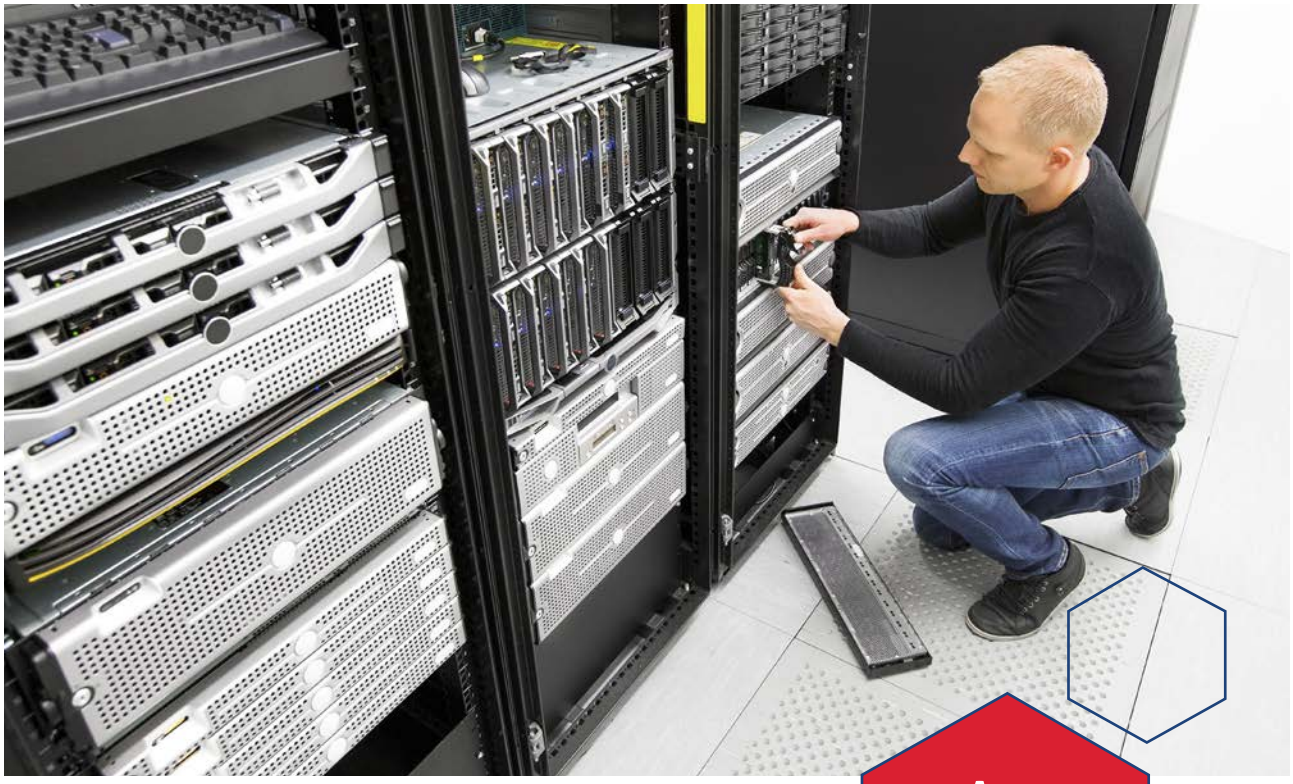
Wussten Sie schon …

Mit der Richtlinie VdS 10005 mit dem Titel „Mindestanforderungen an die Informationssicherheit für Klein- und Kleinstunternehmen“ gibt es auch einen Informationssicherheitsstandard für Einpersonengesellschaften und Handwerker.

Vertrauen Sie einem starken Partner

NESEC ist spezialisierter Anbieter von Lösungen für Ihre Informationssicherheit. Zu unserem Portfolio gehört die umfassende Beratung unserer Kunden in allen Belangen der Informationssicherheit und des Datenschutzes ebenso wie die komplette Erstellung von Sicherheitskonzepten, die Prüfung der Informationssicherheit durch Audits und Penetrationstests und die Installation und Konfiguration Ihrer IT-Sicherheitssysteme.

Gemäß dem Motto „lieber eine Sache richtig als von vielem ein bisschen“ spricht NESEC gezielt die Bedürfnisse mittelständischer Kunden zur Informationssicherheit an.



NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH

Fürholzener Straße 5a
85386 Eching
Telefon: 089 - 45217100
E-Mail: welcome@nesec.de
Internet: www.nesec.de

NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH