ANTARES
NETLOGIX

ANTARES-NETLOGIX

INFORMATIONSSICHERHEIT AUS DER PRAXIS

DI (FH) Gerhard Kratschmar | diplomierter Datenschutzbeauftragter

Antares-NetlogiX Netzwerkberatung GmbH
Feldstraße 13, A-3300 Amstetten
T: +43 74 72 / 65 480-0 E: office@netlogix.at

www.netlogix.at

Informationssicherheit aus der Praxis

Nachdem in den Unternehmen etwas Ruhe in das Thema Datenschutz eingekehrt ist, gibt es nun Zeit, sich weiteren Projekten zu widmen. Die Auseinandersetzung mit technischen und organisatorischen Maßnahmen um personenbezogene Daten zu schützen war doch recht aufschlussreich und vielerorts hörte man von der Geschäftsleitung Aussagen wie **„Wenn wir schon das Sicherheitsniveau von personenbezogenen Daten steigern, dann schützen wir doch auch unsere gesamten Firmendaten!“.**

Die DSGVO und nationale Datenschutzgesetze kümmern sich ausschließlich um personenbezogene Daten. Zusätzlich zu dieser gesetzlichen Verpflichtung ist **Informationssicherheit der freiwillige, gesamtheitliche Schutz aller relevanten Informationen eines Unternehmens.**

Je nach Branche gibt es verschiedene Informationen, die besonders schützenswert sind. Als Beispiele zählen etwa Finanzdaten, technische Zeichnungen, Baupläne und Verträge dazu.

Um sich professionell dem Thema Informationssicherheit zu widmen, empfiehlt es sich, ein Managementsystem aufzubauen, ein sogenanntes ISMS. Als Königsweg gibt es hier die **Normen ISO/IEC 27001 bzw. den deutschen BSI-IT Grundschutz.** Speziell für KMU gibt es übrigens auch sehr einfache Fragenkataloge, die als sogenannte „Quick Wins“ Informationssicherheit aufbauen können.

Ein vollwertiges ISMS erfasst Ihre Infrastruktur in sogenannten Risikoobjekten (Gebäude, Räume, Hardware, Software, ...) und untersucht diese auf mögliche Schwächen. Sicherheit muss im ISMS messbar werden, daher werden Ziele definiert und auch die Einhaltung dieser überprüft. Regelmäßige Berichte an das Management sind ebenfalls Teil des Systems.

ÜBER DEN AUTOR

DI (FH) GERHARD KRATSCHMAR
dipl. Datenschutzbeauftragter

Als ehemaliger Berufspilot ist er gewohnt, strukturiert vorzugehen, Prozesse zu erstellen und diese strikt einzuhalten. Der Schutz von personenbezogenen Daten sowie Safety & Security stehen im Vordergrund.

Eigener CISO?

Doch wer soll all das erledigen? Die IT-Abteilung ist ständig mit Projekten ausgelastet und Fachkräfte zu finden ist derzeit nicht leicht. Nur wenige große Unternehmen leisten sich eine eigene Stelle des „Chief Information Security Officers“ oder auch Informationssicherheit-Koordinators. Antares NetlogiX bietet Ihnen hier entsprechende Unterstützung – nützen Sie unser CISO-Know-how aus unseren Projekten.

Wir bieten Ihnen die Möglichkeit, die Strategie Ihrer **Sicherheitsmaßnahmen** auszulagern und unterstützen Ihr Unternehmen, damit Ihre **Informationssicherheitsprojekte angemessen begleitet werden.** Durch ein regelmäßiges Reporting an die Unternehmensführung werden datenschutzrechtliche und sicherheitsrelevante Vorfälle schnell und zuverlässig kommuniziert.

Wie gehen wir es an?

Nicht immer ist eine Zertifizierung gemäß ISO/IEC 27001 erforderlich. Häufig möchten sich Unternehmen einfach an der Norm orientieren und langsam die verschiedenen Maßnahmen und Kapitel umsetzen, um zu einem späteren Zeitpunkt für das begehrte Zertifikat vorbereitet zu sein. Unser Team orientiert sich an den anerkannten Sicherheitsnormen und erstellt einen individuellen Projektplan für Sie.

So könnte ein Maßnahmenplan aussehen:

JAHR 1 → STEP 1	**JAHR 2** → STEP 2	**JAHR 3** STEP 3
A.5.1.1 Informationssicherheits-richtlinien	A.7.2 Personalsicherheit während der Beschäftigung	A.12 Betriebssicherheit
A.6.2.1 Richtlinie zu Mobilgeräten	A.8.2 Informationsklassifizierung	A.16 Handhabung von Informationssicherheitsvorfällen
A.6.2.2 Telearbeit	A.9 Zugangssteuerung	A.17 Business Continuity Management

Informationssicherheit lässt sich am besten als „Top-Down“-Projekt durchsetzen. Ein gelungener Projektstart benötigt daher die volle Unterstützung der Geschäftsführung.

Ein erfolgreicher Start wäre zum Beispiel die **Ankündigung der IT-Richtlinien und der Awareness-Schulung** bei einem Firmenevent persönlich durch das Management. So wird von Anfang an eine hohe Akzeptanz bei den Mitarbeitern erreicht. Schritt für Schritt setzen wir nun gemeinsam Maßnahmen um, die Ihr Sicherheitsniveau heben.

crisam DECISION ENGINEERING

Für die **Dokumentation des gesamten ISMS empfehlen wir die Software „CRISAM-Explorer“**. Dieses Portal ist modular gestaltet, Sie können auch das Datenschutz-Management oder Unternehmens-Risikomanagement (ERM) hier integrieren.
www..crisam.net/de/crisam-explorer

Und weiter? Mit dem Antares CISO-Service steht Ihnen in einer Stelle ein ganzes Team zur Verfügung. Je nach Aufgabenbereich unterstützen Sie Experten aus dem Bereich IT-Security.

CISO SERVICE

Ob wir Ihren (neuen) CISO bei der Arbeit **begleiten**, Aufgaben nur für einen **vereinbarten Zeitraum** übernehmen (auch als Vertretung), oder ob wir als CISO Ihr Unternehmen **langfristig begleiten** und die Koordination und Überwachung, sowie den Aufbau von Sicherheitsrichtlinien komplett übernehmen, bleibt Ihnen überlassen.

CISO-COACHING
RENT-A-CISO
CISO AS A SERVICE

Risikobewertung & IT-Struktur-Analyse **RISIKOANALYSE** Identifikation kritischer Anwendungen.

Laufende **AUDITIERUNG** zum Stand der Umsetzung und Weiterentwicklung.

Strukturierte **IT-DOKUMENTATION** (Betriebshandbuch, Notfallhandbuch)

Erstellung & Anpassung von **SICHERHEITS-RICHTLINIEN** und Schutzzielen für unternehmenskritische Werte.

Sensibilisierung der Mitarbeiter durch **AWARENESS TRAININGS** & konkrete Kampagnen.

Sicherstellung und Einhaltung der **DSGVO VORGABEN** sowie allen geforderten Maßnahmen.

Etablierung eines Mangementsystems zur **INFORMATIONS-SICHERHEIT (ISMS)** nach ISO 27001 (mit CRISAM)

Etablierung & Verwaltung eines **PORTFOLIO-MANAGEMENTS** der sicherheitsrelevanten Geschäftsprozesse.

ANTARES RED TEAM

Als zusätzliches Service unterstützt Sie das **ANTARES RED TEAM** bei der **SCHWACHSTELLEN-ANALYSE** und bei **INCIDENT RESPONSE TESTS.**

UNSERE EXPERTEN

ISMS-Manager & Auditoren nach ISO27001

DI Alexander Graf

Als technischer Geschäftsführer und ISMS-Manager & Auditor nach ISO 27001 leitet DI Alexander Graf nicht nur das gesamte Team, sondern unterstützt Kunden auch mit seinem umfangreichen Know-how in der Planung und Umsetzung von komplexen IT-Projekten.

Stefan Winkler

Als Leiter des Antares Red Teams sowie ISMS-Manager & Auditor nach ISO 27001 führt Stefan Winkler laufend Security Audits sowie Penetrationtests auf Applikations- & Netzwerkebene durch. Er gilt als einer der führenden PCI DSS-Experten in Österreich.

DI (FH) Gerhard Kratschmar

Als diplomierter Datenschutzbeauftragter, ISMS-Manager & - Auditor nach ISO 27001 und ehemaliger Berufspilot sowie Safety & Security Manager im weltweiten Einsatz, unterstützt Gerhard Kratschmar unsere Kunden vor allem bei der Umsetzung der EU-DSGVO.

ANTARES NETLOGIX

Antares-NetlogiX Netzwerkberatung GmbH
Feldstraße 13, A-3300 Amstetten
T: +43 74 72 / 65 480-0 E: office@netlogix.at

www.netlogix.at

Bildnachweise: © Sergii Figurnyi / fotolia.com (European flags in Brussels / 75936736)