ANTARES NETLOGIX

DATA PROTECTION

AWARENESS

BUSINESS CONTINUITY

COMPLIANCE

CISO AS A SERVICE

COMPLIANCE

Datenschutz-Vorgaben & Business Continuity Management

Wir unterstützen Sie bei der Erfüllung der **gesetzlichen Compliance-Vorgaben** (z. B. PCI DSS, ISO 27001, DSGVO) und Ihrer eigenen Unternehmensrichtlinien. Außerdem integrieren wir das Thema **Business Continuity Management** in Ihre IT-Sicherheitsinfrastruktur.

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

www.netlogix.at

ANLASS FÜR DATENSCHUTZMASSNAHMEN

Ihre Anforderungen

Es gibt viele Gründe, sich für mehr Sicherheit zu entscheiden. Aktuell gibt es fünf große Themen, die Unternehmen empfindlich treffen können. Jede dieser Bedrohungen ist mit hohen Kosten verbunden, bei manchen wird zusätzlich auch die Reputation des Unternehmens geschädigt.

CYBER INSURANCE - PRÄMIENGESTALTUNG

Denken Sie über eine Cyber-Versicherung nach? Achtung! Die Versicherer prüfen zuerst Ihre Infrastruktur und erhöhen bei geringen Sicherheitsstandards die Prämie.

› CYBER INSURANCE 3

SCHADEN DURCH IT-AUSFÄLLE

Ein Ausfall Ihrer IT-Systeme kann Ihren gesamten Betrieb lahmlegen. Gehen Sie kein Risiko ein und sichern Sie sich ab!

› BUSINESS CONTINUITY 4

SCHADEN DURCH BETRUG

Phishing war gestern - heute werden große Fische gejagt. Mit „Whaling" werden ganz gezielt Mitarbeiter aus dem oberen Management geködert. Seien Sie wachsam!

› AWARENESS 5

DSGVO-STRAFPRÄVENTION

Die Datenschutzbehörde kann Strafen bis zu 4 % vom Umsatz verhängen – gehen Sie auf Nummer sicher und stellen Sie Ihr Unternehmen DSGVO-konform auf.

› CISO as a Service 6

SCHADEN DURCH DATENDIEBSTAHL

Ihre Daten sind wertvoll für Ihr Unternehmen - aber auch für den Mitbewerb. Mit unseren Modulen lassen Sie Datendieben keine Chance.

› DATENSCHUTZ-MODULE 7

TIPP VOM DATENSCHUTZBEAUFTRAGTEN

Der Start in die Welt des Datenschutzes ist für viele Unternehmen eine Reise ins Unbekannte. Beginnen Sie mit unseren beiden Workshops auf technischer und rechtlicher Ebene, um eine erste Struktur zu schaffen. In zwei Tagen wird der Ist-Stand Ihrer Infrastruktur und Organisation erfasst und Sie erfahren alle wichtigen Fakten der geltenden Datenschutz-Grundverordnung.

Mit den Ergebnissen dieser beiden Workshops sind Sie gut aufgestellt für die Zukunft. Sie bekommen einen konkreten Zeitplan und eine Liste mit Punkten, die empfohlen bzw. künftig vorgeschrieben sind. Mit dieser Struktur können Sie die nächsten Schritte mit internen Ressourcen oder auch mit bestehenden Partnern umsetzen.

DI (FH) Gerhard Kratschmar

Als diplomierter Datenschutzbeauftragter, ISMS-Manager & - Auditor nach ISO 27001 und vormals Flight Safety Manager unterstützt Gerhard Kratschmar unsere Kunden bei organisatorischen Informationssicherheits- & Datenschutzprojekten.

SO **FUNKTIONIERT'S**

Schritt für Schritt

OHNE CYBER SECURITY KEINE CYBER VERSICHERUNG

IT-Security ist ein bestimmender Faktor für das Risk-Management

Wenn man Fachleute befragt, vom Vorstand bis hin zu Administratoren, dann sind alle Aspekte im grünen Bereich: **Abgesicherte Systeme und Redundanzen** sorgen im technischen Bereich und das **Risk Management** im kaufmännischen Bereich für eine klare Risikoverteilung und -bewertung. Rechtliche und weitere Gefahren aus der Betriebstätigkeit werden beurteilt, versichert oder in Kauf genommen. Soweit so gut. Es gibt aber auch eine Vielzahl von neuen Gefahren, von bisher falsch eingeschätzten Kumulrisiken und auch von gar nicht versicherbaren Bedrohungen.

GLOBALE GESCHÄFTSRISIKEN

Die Folgen von **Betriebsunterbrechungen**, **Cybervorfällen** sowie **Naturkatastrophen** sind die Top-Risiken, mit denen sich Unternehmen befassen müssen.

CYBER-VORFÄLLE
(cyber crime & cyber war, data breach)

BETRIEBSUNTERBRECHUNGEN
(inkl. Lieferkettenunterbrechungen)

NATURKATASTROPHEN
(Klimawandel, Sturm, Hochwasser, etc.)

„Der ‚Blackout' ist nicht versicherbar. Der flächendeckende Ausfall der kritischen Infrastruktur oder des Internets ist nicht kalkulierbar und übersteigt jede mögliche Schadenersatzleistungsfähigkeit."
Jürgen Kolb, Geschäftsführer Antares-NetlogiX Netzwerkberatung GmbH

CYBERCRIME UND CYBERWAR ALS HERAUSFORDERUNG JEDER IT-SECURITY

IT-SECURITY GEWINNT AN BEDEUTUNG

Wenn Sie heute als mittelständisches oder globales Unternehmen nicht über eine eigene IT-Security-Abteilung verfügen, ist eine Beurteilung von Cyber-Gefahren schwer möglich. Selbst wenn diese State-of-the-Art Softwarelösungen einsetzt und sehr gut geschult ist, liegt der Fokus immer auf einer hochverfügbaren Verteidigungsbereitschaft. Zwangsläufig sind offensive und aggressive Vorgehensweisen – wie sie Hacker und Eindringlinge nutzen - nicht im Blickfeld.

Konkrete Business-Mehrwerte eines starken IT (Security) Partners

- Voraussetzung für anspruchsvolle Cyber-Risiko-Versicherung
- Senkung der Risiken für das Management (Haftpflichtversicherungen)
- Senkung der Kosten im Schadensfall (Imageschäden, Datenverlust, Gerichtsverfahren)
- Optimierung der Performance, Redundanzen und Resilienz von Unternehmen
- Überlebensfähigkeit der Organisation steigt erheblich (Krisen, Naturkatastrophen, Skandale)
- Innovationsbereitschaft und Zukunftssicherheit ist ohne IT unmöglich

BUSINESS CONTINUITY MANAGEMENT

Für den Ernstfall bestens gewappnet!

Unvorhergesehene Ereignisse nicht nur hierzulande, sondern auch in Produktions- oder Beschaffungsländern, können die Geschäftsprozesse eines Unternehmens erheblich stören. Solche Schäden von Unternehmen zu minimieren und bestmögliche Vorkehrungen für den Fall gravierender Störungen zu treffen ist Ziel von **Business Continuity Management Systemen (BCMS).**

PROTECTION

Schützen Sie sich vor **direkten Angriffen** auf die Organisation aus wirtschaftlichen, sozialen und/oder politischen Gründen. Minimieren Sie das Risiko eines **Datenverlustes** und vermeiden Sie kostenintensive **Ausfallzeiten**.

INCIDENTS

Schutz vor **unkalkulierbaren Ereignissen** wie zum Beispiel Naturkatastrophen, technische oder menschliche Fehler. Ob soziale oder globale Gefahren - **jeder Vorfall ist mittlerweile IT-relevant!**

STANDARDS

Halten Sie **Vorgaben und Regularien** von Zulieferern, Kunden, Gesetzgeber & Wirtschaftsprüfern ein. Vermeiden Sie kostenintensive **Haftungs- und Schadensersatzfragen**.

SO **FUNKTIONIERT'S**

Wir sorgen für einen 360° Ansatz

Wir verfügen über umfangreiches Know-how und ermöglichen Ihnen eine durchgängige Integration des BCM-Prozesses in Ihre IT.

- Wir beginnen beim **Notfallhandbuch**, übernehmen bestehende Prozesse und bilden diese ab.
- Die Shutdown/Wiederanlauf-Prozeduren werden mit **iQSol PowerApp** ermöglicht.
- Die Notfallkommunikation erfolgt über den **iQSol Alert Messaging Server**.
- Die vorhandene IT Security kann mit **iQSol LogApp** konzentriert und korreliert werden.
- Zusätzlich kooperieren wir mit I**T-Fachanwälten** und setzen auf eigene **Organisations- und Projektspezialisten** sowie Security- und Netzwerkexperten. Damit ist ein konstanter Prozess garantiert.

NOTFÄLLE PASSIEREN NICHT

- solange man vorgesorgt hat!

Wir wissen, dass ein permanentes und stets aktuell gehaltenes Business-Continuity-Konzept nicht einfach und nicht für jede IT-Umgebung „durchzuhalten" ist. Wir beraten Sie unverbindlich und setzten gemeinsam den BCM-Prozess auf. Auf Wunsch betreiben wir diesen für Sie in Ihrem Sinne als **Managed Security Service**.

SECURITY AWARENESS

Schaffen Sie Bewusstsein!

Das Thema Security Awareness spielt in Unternehmen oft eine untergeordnete Rolle, da die Bedeutung in den meisten Fällen unterschätzt wird. Die Erfahrung zeigt jedoch, dass technische Maßnahmen nur bis zu einem gewissen Grad die Informationssicherheit verbessern können. **Trotz technischer Maßnahmen bleibt der Mensch immer das größte Sicherheitsrisiko.**

WIR HABEN DIE ERFAHRUNG
Schaffen Sie Bewusstsein für Sicherheit!

Mit unserem **Security Awareness Programm** unterstützen wir Sie bei der Erstellung von einfach verständlichen **Sicherheitsrichtlinien** und der **Bewusstseinsbildung** Ihrer Mitarbeiter/innen. Machen Sie das schwächste Glied in der Security-Kette zu Ihrer stärksten Abwehr!

WARUM AWARENESS WICHTIG IST

Unsere Experten verraten Ihnen wie einfach es ist, Daten und Informationen zu erhalten.

- „Mit dunklem Anzug, Brille, strenger Miene und einer Visitenkarte eines globalen Wirtschaftstreuhänder-Konzerns kommen Sie fast überall hinein!" **Dr. Wolfgang Zuser**
- „In der Luftfahrt ist ein Awareness-Training seit Jahrzehnten fixer Bestandteil der Pilotenausbildung. Nur im perfekten Zusammenspiel zwischen Mensch und Technik lässt sich die Sicherheit weiter steigern." **DI (FH) Gerhard Kratschmar, CISSP**

UNSERE AWARENESS PAKETE

Setzen Sie den ersten Schritt für ein erfolgreiches Security-Awareness-Konzept mit unserem Basispaket!

BASISPAKET

SICHERHEITSRICHTLINIEN I

Inhalte:

+ Überprüfung der bestehenden Sicherheitsrichtlinien
+ Ausarbeitung von verständlichen Vereinbarungen zwischen Mitarbeiter und Unternehmen
+ Handlungshinweise für die Praxis
+ inkl. Halbtagesworkshop zur Anpassung

SICHERHEITSRICHTLINIEN II

Die Erweiterungsmodule liefern praktische Handlungsanweisungen zum Thema und benötigen das Basispaket.

+ Passwörter
+ Soziale Netze
+ USB-Sticks

TRAINING

SECURITY AWARENESS TRAINING (max. 12 Teilnehmer)

+ inkl. Vorbesprechung und Nachbereitung
+ Individuelle Zielgruppenanpassung (z. B. Geschäftsführung, HR-Abteilung, Buchhaltung, Produktionsmitarbeiter etc.)

Trainingsinhalte:
Bedrohungsszenarien, Passwörter, E-Mail Unsicherheiten, Rollenspiele mit Betrugssimulation, Beispiele aus der Praxis

INFORMATION

AWARENESS NEWSLETTER

Vorgefertigte Newsletter zu den Themen: Passwörter, Soziale Netze, USB-Sticks

+ Mitarbeiter erhalten 4x im Jahr Informationen zur Handhabung.

INFORMATION

STRATEGIEWORKSHOP

Sicherheitsbewusstseins Ist-Analyse, Bewertung aktueller Maßnahmen, Ausarbeitung von Maßnahmenpaketen

ANLX.CLOUD AWARENESS & eLEARNING SERVICE

Mit unserem Service unterstützen wir Sie mit einer 3D-Online-Schulungsplattform bei Schulungsmaßnahmen. Wir übernehmen für Sie die Zusammenstellung des Schulungsprogramms, die Umsetzung und die gesamte Kursverwaltung.

CHIEF INFORMATION SECURITY OFFICER

Standards & Vorschriften einhalten

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.

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 Schutzziele für unternehmenskritische Werte.
Sensibilisierung der Mitarbeiter durch **AWARENESS TRAININGS** & konkrete Kampagnen.	Sicherstellung und Einhaltung der **DSGVO VORGABEN** sowie aller geforderten Maßnahmen	Etablierung eines Managementsystems zur **INFORMATIONS-SICHERHEIT (ISMS)** nach ISO 27001	Etablierung & Verwaltung eines **PORTFOLIO-MANAGEMENTS** der sicherheitsrelevanten Geschäftsprozesse.

CISCO-COACHING
RENT-A-CISCO
CISCO AS A 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.

UNSERE EXPERTEN

ISMS-Manager & - Auditoren nach ISO27001

ANTARES RED TEAM

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

DI Alexander Graf, CISSP

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, CISSP

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 er als einer der führenden PCI DSS-Experten in Österreich.

DI (FH) Gerhard Kratschmar, CISSP

Als diplomierter Datenschutzbeauftragter, ISMS-Manager & -Auditor nach ISO 27001 und vormals Flight Operations Safety & Compliance Manager unterstützt Gerhard Kratschmar unsere Kunden bei organisatorischen Informations-sicherheits- & Datenschutzprojekten.

- **KOMPETENZ & KNOW-HOW:** Unsere Experten verfügen über jahrelange Erfahrung aus vielen IT-Projekten, organisatorisches Wissen und eine kaufmännische Ausbildung.
- **UNABHÄNGIG & OBJEKTIV:** Durch die Übertragung der Kontrollfunktion erreichen Sie ein Höchstmaß an Unabhängigkeit und vermeiden potenzielle Betriebsblindheit.
- **KOSTENGÜNSTIG & PLANBAR:** Durch Expertensharing entsteht ein optimales Preis-Leistungs-Verhältnis. Viele Unternehmen benötigen die Funktion eines CISO oft nur wenige Tage oder Monate.

MODULÜBERSICHT

Schritt für Schritt zur DSGVO

Unsere Beratung und Unterstützung startet stets mit einem **Datenschutz-Workshop** und einer entsprechenden **Analyse der aktuellen Situation**. Danach stehen wir Ihnen bei der Ausarbeitung der Umsetzungsstrategie zur Seite und helfen Ihnen, die notwendigen **Maßnahmen anhand unseres modularen Aufbaus** Schritt für Schritt umzusetzen.

1. VERSCHLÜSSELUNG

1.1	E-Mail-Verschlüsselung
1.2	Datei-Verschlüsselung
1.3	Datenbank-Verschlüsselung
1.4	Cloud-Verschlüsselung

2. VERTRAULICHKEIT

2.1	Identitäts- & Berechtigungsmanagement
2.2	Datenschutzkonforme Protokollierung
2.3	System-Integritäts-Monitoring
2.4	Enterprise-Passwort-Management
2.5	Netztrennung/Zugangskontrolle
2.6	Privileged Access Management
2.7	Multifaktor-Authentifizierung
2.8	Schnittstellensicherheit

3. INTEGRITÄT

3.1	Wiederanlauf Rechenzentrum
3.2	Wiederanlauf Hub-Location
3.3	Datenarchivierung
3.4	Datenwiederherstellung
3.5	Advanced Threat Protection
3.6	Schwachstellen-Management
3.7	Patch-Management

4. VERFÜGBARKEIT

4.1	Co-Location
4.2	Geo Load Balancing
4.3	Failover-Architektur
4.4	Betriebshandbuch
4.5	Notfallhandbuch

5. QUALITÄTSSICHERUNG IM BETRIEB

5.1	Datenschutz-(Re-)Audit
5.2	Verfügbarkeits- und Infrastruktur-Audit
5.3	(regelmäßige) Risiko-Analyse
5.4	Forensische Analyse und Bewertung
5.5	(regelmäßige) Failover/Disaster-Test

6. COACHING & SCHULUNG

6.1	(externer) Datenschutzbeauftragter
6.2	Schulung Datenschutzbeauftragter
6.3	Erstellung von Datenschutzrichtlinien
6.4	Datenschutz Folgeabschätzungen
6.5	Verfahrensverzeichnis
6.6	Softwareentwicklung „privacy by design“

7. AWARENESS

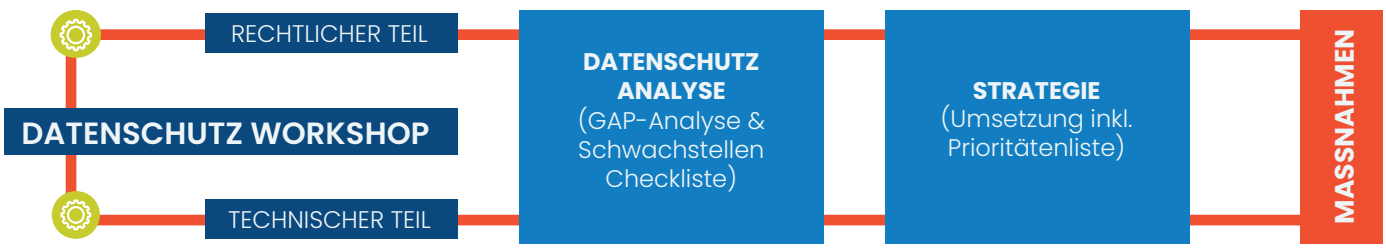
7.1	Sicherheitsrichtlinien
7.2	Security-Awareness-Strategie
7.3	Security-Awareness-Training
7.4	Security-Awareness-Newsletter

8. CLOUD SERVICES & OUTSOURCING

8.1	Vertragsaudit bestehender Leistungen
8.2	Vertragsaudit DSGVO-Konformität
8.3	Technischer Infrastruktur-Audit
8.4	Technischer Security-Audit

SO **FUNKTIONIERT'S**

Schritt für Schritt



EU-DSGVO: GESETZESANFORDERUNGEN

Mit unseren Modulen decken Sie folgende Gesetzesanforderungen ab:

EU-DATENSCHUTZ-GRUNDVERORDNUNG	MODULE	
Artikel 25 – Datenschutzfreundliche Voreinstellungen	6.6	Softwareentwicklung „privacy by design“
Artikel 28 – Auftragsverarbeiter	8.1 8.2 8.3 8.4	Vertragsaudit bestehender Leistungen Vertragsaudit DSGVO-Konformität Technischer Infrastruktur-Audit Technischer Security-Audit
Artikel 30 – Verarbeitungstätigkeiten	6.5	Erstellung Verfahrensverzeichnis
Artikel 32 (1) (a) Pseudonymisierung und Verschlüsselung	1.1 1.2 1.3 1.4	E-Mail-Verschlüsselung Datei-Verschlüsselung Datenbank-Verschlüsselung Cloud-Verschlüsselung
Artikel 32 (1) (b) Vertraulichkeit sicherstellen	2.1 2.2 2.4 2.7 2.8	Identitäts- & Berechtigungsmanagement Datenschutzkonforme Protokollierung Enterprise Passwort Management Multifaktor-Authentifizierung Schnittstellensicherheit
Artikel 32 (1) (b) Integrität sicherstellen	2.3 2.6 3.1 3.2 3.3 3.4 3.5 3.6 3.7	System-Integritäts-Monitoring Privileged Access Management Wiederanlauf Rechenzentrum Wiederanlauf Hub-Lokation Daten-Archivierung Daten-Wiederherstellung Sandboxing Schwachstellen-Management Patch-Management
Artikel 32 (1) (b) Verfügbarkeit / Belastbarkeit der Systeme und Dienste **Artikel 32 (1) (c)** Wiederherstellung der Daten und des Zugriffs darauf bei technischem oder physischem Zwischenfall	4.1 4.2 4.3 4.4 4.5	Co-Location Geo Load Balancing Failover-Architektur Betriebshandbuch Notfallhandbuch
Artikel 32 (1) (d) Regelmäßige Überprüfung der Maßnahmen	5.1 5.2 5.5	Datenschutz-(Re-)Audit Verfügbarkeits- und Infrastruktur-Audit Failover/Desaster-Test
Artikel 32 (2) Risikobewertung	5.3	Risikoanalyse
Artikel 32 (4) Sicherstellung, dass personenbezogene Daten nur auf Anweisung verarbeitet werden.	2.1 2.2 2.4 2.6 6.3	Identitäts- & Berechtigungsmanagement Datenschutzkonforme Protokollierung Enterprise-Passwort-Management Privileged Access Management Erstellung von Datenschutz-Richtlinien
Artikel 33 Meldungen von Verletzungen an die Aufsichtsbehörde	5.4	Forensische Analyse und Bewertung
Artikel 33 (5) Dokumentation der Verletzungen inkl. aller Fakten zur Überprüfung durch die Aufsichtsbehörde	2.2 5.4	Datenschutzkonforme Protokollierung Forensische Analyse und Bewertung
Artikel 35 (1) Abschätzung für neue Verarbeitungsvorgänge	6.4	Datenschutz Folgeabschätzung
Artikel 37 - Datenschutzbeauftragter	6.1 6.2	Externer Datenschutzbeauftragter Schulung Datenschutzbeauftragter
Artikel 47 – Verbindliche interne Datenschutzvorschriften	6.1 6.2 6.3 6.4 7.1 7.2 7.3 7.4	Externer Datenschutzbeauftragter Schulung Datenschutzbeauftragter Erstellung Datenschutzrichtlinien Datenschutz Folgeabschätzung Sicherheitsrichtlinien Security-Awareness-Strategie Security-Awareness-Training Security-Awareness-Newsletter

ANTARES NETLOGIX

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