DATA PIE

DATA PIE® CYBERSECURITY SECURITY CHECK

DATA PIE

DATA PIE® CYBERSECURITY AG
JÖCHLERWEG 2/4, 6340 BAAR

+41 (0) 501 60 85
info@data-pie.com

INHALTSVERZEICHNIS

Einführung

Die **Data Pie® Cybersecurity AG** engagiert sich International für die Umsetzung der Informationssicherheit mit dem **Bundesamt für Sicherheit in der Informationstechnik** und der **AXA Gruppe Schweiz**. In Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI®), wurde ein Verfahren zur Reduzierung von IT-Risiken entwickelt. Das Verfahren sichert Schwachstellen und rechtliche Umsetzungen im Datenschutz ab. Um die IT-Sicherheit möglichst umfassend abzudecken, überprüft der **Data Pie® - Security Check** die folgenden drei Bereiche:

- technische/anwendbare IT-Sicherheit
- rechtliche Anforderungen
- IT-Risikomanagement

Mit diesen Leistungen schliesst die Data Pie® Cybersecurity AG eine Lücke, die herkömmliche Kanzleien und Cybersecurity Firmen nicht schliessen und bietet eine umfangreiche Variante an, die einen überteuerten Penetrationstest in vielen Fällen überflüssig macht.

Folgende Ergebnisse liegen nach dem Security Check vor:

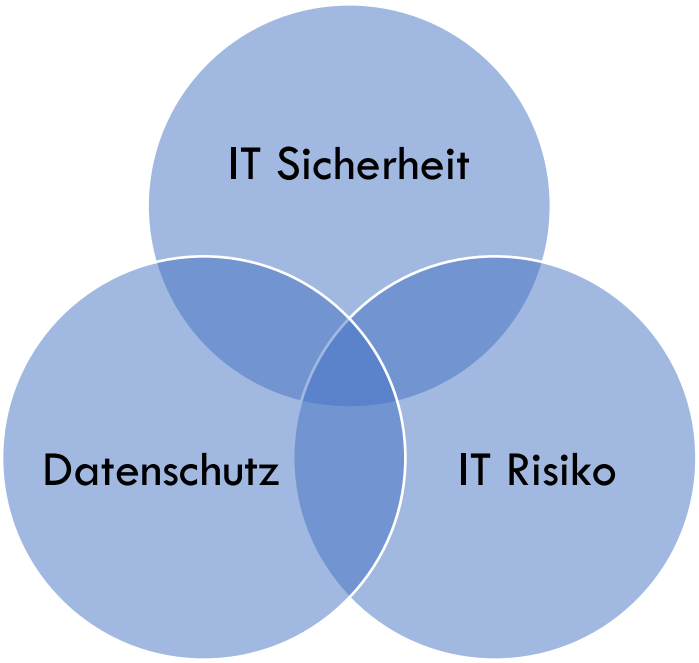
- Technischer IST-Zustand
- Abweichungen des IST-Zustands zu internationalen Standards sind bekannt
- Rechtliche Anforderungen zum Datenschutz sind geprüft und bekannt
- Ergebnisse sind in einem Bericht festgehalten

Weitere Vorteile:

- Nach erfolgreicher Umsetzung der empfohlenen Massnahmen, erhalten Kunden ein Security Check-Label, mit denen sie Vergünstigungen und einen unkomplizierten Einstieg in eine Cyberversicherung bei der AXA Gruppe erhalten.
- Die angefallenen Kosten sind an weitere Dienstleistungen anrechenbar.

Leistungsumfang des Security Check

Dieser Abschnitt gibt einen Überblick über die im Rahmen des Data Pie® Security Check erbrachten Leistungen. Das Ziel ist es, Schwachstellen in der aktuellen Informationssicherheitsstrategie und der bisherigen Umsetzung von ergriffenen Massnahmen aufzuzeigen.



Anwendbare/Technische IT-Sicherheit

In der anwendbaren/technischen Informationssicherheit geht es um die drei Schutzziele: die Vertraulichkeit, Integrität und Verfügbarkeit von Daten. Es werden technische und organisatorische Massnahmen angewendet, um Systeme vor Cyberangriffen und anderen Bedrohungen zu schützen. Dazu zählen zum Beispiel Zugriffskontrollen, Kryptographie, Zugangsmanagement, Firewalls, Proxies, aktuelle Versionen, Operation Security (OPSec) und einige weitere. Diese testen wir im multi-tool Verfahren.

Datenschutz (Rechtliche Sicherheit)

Die rechtliche Sicherheit ist meist durch Konsequenzen von nicht eingehaltenen rechtlichen Anforderungen gefährdet. Der Bund passt das Datenschutzgesetz und Informationssicherheitsgesetz kontinuierlich den wachsenden Bedrohungen in der Informationssicherheit an. Für die Einhaltung der rechtlichen Anforderungen ist jedes Unternehmen selbst verantwortlich und trägt alleinig das volle Risiko bei einem Schadensfall. Den notwendigen Schutz bietet eine vollständige und aktuelle Datenschutzbestimmung und gegebenenfalls eine Cyberschutz-Versicherung.

In unserem Security Check überprüfen wir Ihre Datenschutzerklärung auf Kompatibilität mit den geltenden Datenschutzgesetzen und kontrollieren das Impressum, der Cookie-Banner sowie das Tracking für Marketingzwecke. Verstösse oder rechtliche Nonkonformitäten werden hervorgehoben und geeignete Beispiele werden im Bericht mitgegeben.

IT-Risikomanagement

Im IT-Risikomanagement werden umfassende, strategische und technische Massnahmen berücksichtigt. Diese werden mit Dokumentationen und Zielsetzungen umgesetzt. Hierbei wird vor allem auf die Wirtschaftlichkeit geachtet, dass wichtige Geschäftsprozesse und Unternehmenswerte geschützt werden. Im Notfall ist ein schnelles Handeln erforderlich. Mit einem passenden Risikomanagement, gewinnen Sie wertvolle Zeit und können Reputationsschäden schon frühzeitig entgegenwirken.

Im Rahmen unseres Security Checks erfassen, strukturieren und bewerten wir mit einer Bedrohungsanalyse die verschiedenen Bedrohungen systematisch für Ihre IT-Systeme und IT-Prozesse.

Diese Risiken werden für jedes Unternehmen individuell identifiziert und nach Schadensausmass sowie nach der Eintrittswahrscheinlichkeit bewertet. Wenn ein Unternehmen bestimmte Risiken nicht übernehmen kann, wird bestimmt, ob und wie diese Risiken minimiert werden können.

IHR PARTNER

Data Pie® Cybersecurity AG ist eine Schweizer Firma mit Sitz im Kanton Zug. Als Partner für die Bundesregierung stehen wir ganz oben auf der Liste für Professionalität, Zuverlässigkeit und führenden Lösungen in der Informationssicherheit.
Zudem sind wir als Trustpartner der AXA Gruppe die einzige IT-Sicherheitsfirma der Schweiz, die Beratungen für AXA-Kunden in der IT-Sicherheit anbietet.

Unsere Experten in der IT-Sicherheit haben alle erforderlichen Ausbildungen, um Ihre IT-Infrastruktur sorgfältig zu prüfen.

GRUNDLAGEN UND METHODIK

Das verwendete Verfahren von der Data Pie® Cybersecurity AG, kommt aus der militärischen Praxis und nennt sich «Cyber Kill Chain».
Der Fokus der Cyber Kill Chain liegt in der Erkennung von hochentwickelten, hartnäckigen Bedrohungen und effektiven Handlungsmassnahmen zur Abwehr von sorgfältig geplanten Cyberangriffen.

Hintergrund unseres Vorgehens

Für die Durchführung der Sicherheitsanalyse orientieren wir uns an den Standards vom BSI® und dem NIST Framework. Die Sicherheitsanalyse wird weltweit in fünf Bereiche unterteilt (identifizieren, schützen, erkennen, reagieren, wiederherstellen, Abbildung unten).
Der **BSI-Standard** ist eine Empfehlung des **deutschen Bundesamtes für Sicherheit in der Informationstechnik**, um die praktische IT-Sicherheit umzusetzen. Das **NIST-Framework** ist ein Leitfaden vom **National Institute of Standards and Technology**, einer Bundesbehörde der Vereinigten Staaten, und dient hauptsächlich zur Verbesserung der cybersicherheitskritischen Infrastrukturen.
Durch die Vielzahl von unterschiedlichen Standards des NIST Frameworks im Bereich Schützen/Protect, ist ein potenzielles Risiko für eine lückenhafte Umsetzung im Gesamtbild möglich. Deshalb richtet sich die Data Pie® Cybersecurity AG für die Umsetzung des Bereiches Schützen/Protect nach dem BSI-Standard.
In den übrigen Bereichen stellt das NIST Framework in der Schweiz eine Best Practice dar. Vom **Schweizer Bundesamt für wirtschaftliche Landesversorgung** wurde der IKT-Minimalstandard für kritische Infrastrukturen entwickelt. Dieser beruht grösstenteils auf dem Reagieren/Respond vom **NIST Framework** und wird auch von der **FINMA** als Audit Grundlage verwendet.

DATA PIE

NIST FRAMEWORK

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Identifizieren: Entwicklung des Verständnisses zur Verwaltung von Cyber-Risiken bezüglich Werte, Daten und Funktionen. Die Identifikation legt den Grundstein für einen effektiven Einsatz.

Schützen: Entwicklung und Umsetzen entsprechender Sicherheitseinrichtungen, um die Leistungserbringung zu gewährleisten. Der Schutz begrenzt mögliche Cyberangriffe.

Erkennen: Entwicklung und Umsetzung entsprechender Massnahmen zur Erkennung von Cyber-Ereignissen. Die Erkennung allein ermöglicht die rechtzeitige Entdeckung von Cyber-Vorfällen.

Reagieren: Entwicklung und Umsetzung entsprechender Massnahmen zur angemessenen Reaktion auf Cyberangriffe. Die Reaktionsfähigkeit unterstützt die Fähigkeit, den Auswirkungen eines möglichen Cyber Ereignisses entgegenzuwirken.

Wiederherstellen: Entwicklung und Umsetzung entsprechender Massnahmen zur Wiederherstellung eines stabilen Zustandes nach einem Cyber-Ereignis. Die Wiederherstellung ermöglicht die ungestörte Wiederaufnahme des Betriebes.

PROJEKTVORGEHEN

Data Pie® - Security Check

Beim **Kickoff Meeting** besprechen wir die Rahmenbedingungen für unser Vorgehen und die Details zum Security Check. Anschliessend wird ein **NDA** und ein **Haftungsausschluss** unterzeichnet, damit alle vorrangigen Informationen wie Dokumentationen und IP-Adressen von der IT-Infrastruktur versendet werden können. (Den Plan der IT-Infrastruktur benötigen wir, falls wir ins IT-System eindringen sollen.)

Der Penetrationstest findet an einem vorab definierten Termin statt und wird remote aus unserem Büro in Baar durchgeführt. Die Analyse des Netzwerks erfolgt im Multi-Tool Verfahren und beginnt mit einer umfangreichen Informationserhebung (OSINT) über Ihre Organisation, Infrastruktur und die vorhandenen Systeme, um alle möglichen Angriffsvektoren zu identifizieren. Danach wird mit öffentlichen sowie mit eigenen Skripten nach Schwachstellen gescannt und die Analyse mit gezielten manuellen Techniken fortgeführt.
Basierend auf den gefundenen Sicherheitslücken und deren Risiko wird ein Abschlussbericht mit empfohlenen Massnahmen zur Behebung aller Risiken ausgehändigt.

Zusätzliche Informationen:

- Aktuelle OWASP Top-10
- Verwendete Tools im multi-tool Verfahren
    - Suchmaschinen (Google, Bind, Yandex, Baidu, Deepsearch, Ahima)
    - Kali Linux Plattform (alle Tools)
    - Maltego
    - Burp Suite
    - Owasp Zap
    - Zenmap
    - Eigene Bibliothek mit zahlreichen, selbstgeschriebenen Skripts

KOSTEN

POS.	ANZ.	BESCHREIBUNG	BETRAG
001	01	Data Pie® - Security Check Folgende Tätigkeiten sind geplant: Kickoff und Planung • OSINT Recherche • Sichtung der Dokumente • Durchführung des Penetrationstests an bis zu 5 IP-Adressen • Überprüfung des Datenschutzes • Verfassung des Berichtes	3´500.00

GESCHÄFTSBEDINGUNGEN

Sie finden alle Produktbeschreibungen auf unserer Website data-pie.com
Die Allgemeinen Geschäftsbedingungen der Data Pie® Cybersecurity AG sind Bestandteil dieses Angebotes.

Preise:	Alle Preise verstehen sich netto, zuzüglich Mehrwertsteuer.
Lieferfrist / Start des Mandates:	2 – 4 Wochen ab Bestellung. (Lieferung bei Zahlungseingang)
Zahlungsbedingungen:	Zahlungskondition ist jeweils 30 Tage netto.
Gültigkeit:	30 Tage

BESTELLUNG

Haben Sie Interesse? Dann kontaktieren Sie uns unter info@data-pie.com

Data Pie Cybersecurity AG
Jöchlerweg 2/4
6340 Baar
www.data-pie.com