InfoGuard
SWISS CYBER SECURITY

Whitepaper – Cyber Risk Management

So behalten Sie Ihre Cyberrisiken im Griff

Kaum ein Tag vergeht, an dem man in den Medien nicht über erfolgreiche Angriffe im In- und Ausland erfährt. Obschon immer neue Security-Lösungen auf dem Markt erscheinen, nehmen die Cyberattacken nicht ab. Cyberrisiken sind omnipräsent.

Cyber Risk Management wird immer wichtiger und muss vom operativen Underdog stärker in das Sichtfeld der Geschäftsleitung verschoben werden. Denn die Verantwortung für die Cyber Resilience eines Unternehmens auch von Cyberrisiken liegt bei der Geschäftsleitung. Der Verwaltungsrat wiederum trägt die Gesamtverantwortung für das Risikomanagement im Unternehmen. Wie Sie ein effizientes und gutes Cyber Risk Management aufbauen können, erfahren Sie in diesem Whitepaper.

INHALTSVERZEICHNIS

1 CYBER RISK MANAGEMENT SCHAFFT TRANSPARENZ

Täglich gibt es neue Cyberattacken auf Unternehmen. Cyber Security ist deshalb ein enorm wichtiges Thema für den Geschäftserfolg eines Unternehmens. Allgegenwärtige Themen wie die Cloud, die Mobilität, das Homeoffice, die Virtualisierung, das «Internet der Dinge», Blockchain etc. sorgen aber für immer neue Herausforderungen und Bedrohungen im Security-Ökosystem. Cyber Security muss natürlich einerseits die klassischen Risiken wie zielgerichtete Malware, Datenverlust, Sicherheitsupdates, starke Authentifizierung, Zugriffsrechte usw. bewältigen. Andererseits ergeben sich auch immer neue anspruchsvolle Aufgaben, die neue Technologien und damit auch Risiken mit sich bringen. Darüber hinaus gilt es, zahlreiche regulatorische Vorgaben wie beispielsweise die E-DSG, resp. die DSGVO zu erfüllen. Die Verantwortung hierbei liegt beim Management. Also bei Ihnen!

Leben ohne Risiko gibt es nicht, weder im privaten Umfeld noch im Geschäftsleben. Risiken, deren Einschätzung und ihre Absicherung bestimmen viele Bereiche unseres Lebens. Vor allem in der Cyber-Welt, denn hier existieren zahlreiche Risiken, die grosse Schäden zur Konsequenz haben können. Die täglichen Meldungen über Datendiebstahl oder Hackerangriffe verdeutlichen dies immer wieder. Gleichzeitig agieren Unternehmen heutzutage in einem komplexen, hochdynamischen und nicht selten globalen Umfeld. Dadurch steigen die Anforderungen an das Risikomanagement sowie das interne Kontrollsystem stetig an. Regulatorischer Druck, Wettbewerbsveränderungen, Compliance-Vorgaben, Cyberkriminalität und die wachsende Infrastruktur-Komplexität – dies sind nur einige der grossen Treiber. Deren Management und Auswirkung auf Risiken und Compliance sind zwei der grössten Herausforderungen, mit denen sich Unternehmen auseinandersetzen müssen.

1.1 Risikomanagement als Teil der Unternehmensführung

Die drei wichtigsten Handlungsfelder eines Unternehmens für eine erfolgreiche Führung sind Governance, Risk und Compliance oder kurz GRC. Dabei versteht man GRC als integrativen, holistischen Ansatz für ein organisationsweites Risikomanagement, Compliance (Einhaltung von Vorschriften) und Governance (Lenkung und Überwachung). Dadurch soll gewährleistet werden, dass die Organisation sich ethisch, ihrem Risikoappetit entsprechend und nach internen sowie externen Vorgaben verhält. Das Ziel dieser Vorgehensweise ist es, durch die Abstimmung von Strategien, Prozessen und Technologien die Effizienz sowie Effektivität zu steigern.

Das Risikomanagement ist ein fortlaufender Prozess, welcher die Erkennung und Bewertung von Risiken sowie die Planung und Umsetzung von Massnahmen in den unterschiedlichen Geschäftsbereichen und -prozessen umfasst. Ebenfalls berücksichtigt wird die ganzheitliche Optimierung des Risikomanagements im Unternehmen.

Wir sind uns sicher, Sie sind sich der Notwendigkeit bewusst, Risiken und Chancen zu steuern, welche Ihre Strategien beeinflussen. Sie unternehmen bestimmt bereits heute erhebliche Anstrengungen, um potenzielle Bedrohungen abzuwenden, die das Erreichen der strategischen Ziele gefährden könnten. Trotzdem – können Sie mit gutem Gewissen sagen, dass Sie bezüglich Cyberrisiken an alles gedacht haben? Falls nicht, helfen wir Ihnen gerne dabei!

Unsere Tipps für Ihr Cyber Risk Management:

1. Richten Sie das Risikomanagement an den Zielen und Vorgaben der Organisation aus.

2. **Identifizieren Sie Risiken**. Ermitteln Sie systematisch alle auf eine Organisation einwirkenden (internen und externen) Risiken, welche die erfolgreiche Erreichung der Ziele und Vorgaben beeinträchtigen könnten. Listen Sie diese auf.

3. **Bewerten Sie die Risiken**. Analysieren Sie die identifizierten Risiken hinsichtlich ihrer Eintrittswahrscheinlichkeit und deren möglichen Auswirkungen. Vergleichen Sie die Risiken mit zuvor festgelegten Kriterien der Risiko-Akzeptanz, um die Prioritäten für die Reaktion auf die Risiken zu priorisieren.

4. Entscheiden Sie sich für die **Risikobehandlungsstrategie**. Definieren Sie, wie mit Risiken auf Grundlage der Risikobereitschaft umgegangen werden soll: Soll ein Risiko aufgrund seiner Bewertung akzeptiert, vermieden, reduziert, verteilt oder übertragen werden?

5. **Kontrollieren Sie die Risiken**. Überwachen Sie die identifizierten und aktuellen Risiken auf Veränderungen gemäss vordefinierten Risiko-Indikatoren. Kontrollieren Sie, ob die Massnahmen erfolgreich gewesen sind.

6. Stellen Sie eine adäquate **Risikokommunikation** sicher. Kommunizieren Sie die Risiken und Risikoergebnisse transparent und nachvollziehbar – zuhanden der Interessengruppen, zur Entscheidungsfindung und als Information.

1.2 Risikomanagement ist eine Managementaufgabe

Gemäss OR 716a ist Risikomanagement eine implizite Aufgabe des Verwaltungsrates. Mit den Revisionen (2008 und 2013) wurden zudem das Interne Kontrollsystem (IKS) und der Risikobericht explizit im Obligationenrecht vorgeschrieben. Die Empfehlungen des Swiss Code gehen mit der weiter gefassten Definition des IKS noch stärker Richtung umfassendes Risikomanagement. Dies beinhaltet alle Tätigkeiten zur Identifikation, Einschätzung, Steuerung und Überwachung von Risiken bezüglich der Zielerreichung im Unternehmen. Es betrachtet sowohl finanzielle, operative (beispielsweise Cyberrisiken) sowie strategische und marktspezifische Risiken.
Obwohl das Risikomanagement nicht explizit als Aufgabe des Verwaltungsrates genannt wird, ist dieser aufgrund der nicht delegierbaren gesetzlichen Aufgaben wie Rechnungslegung, Finanzkontrolle, Überwachung etc. verantwortlich. Der Verwaltungsrat hat folgende Aufgaben:

- Gesamtverantwortung für das Risikomanagement im Unternehmen
- Definiert die Risikostrategie
- Periodische Überprüfung des Risikoprofils
- Trägt die Verantwortung für die Festlegung und Überwachung des internen Kontrollsystems
- Durchführung einer Risikobeurteilung und Berichterstattung im Lagebericht.

Seit der Aktienrechtsrevision 2008 trägt der Verwaltungsrat zudem die Verantwortung, dass ein internes Kontrollsystem existiert. Seit 2013 müssen ordentlich revisionspflichtige Unternehmen anstelle des Jahresberichts einen Lagebericht mit einer Risikobeurteilung erstellen.

1.3 Cyber Risk Management ist Teil der Corporate Resilience

Als Teil des Managements haben Sie verschiedene Aufgaben im Bereich der Cyber Resilience. Eine davon ist es, für jede Art von Risiken, die Ihr Unternehmen treffen könnten, adäquate Massnahmen zur Steuerung zu definieren und die Wirksamkeit dieser Massnahmen permanent zu überwachen. Dieses Unternehmens-Risiko-Management ist Teil der Corporate Resilience. Sie müssen schlussendlich die **Risiken identifizieren, bewerten und steuern** sowie die Risiko-Strategie (Risikoappetit) festlegen. Insofern kommt der Risiko-Strategie sowie der Auswahl von geeigneten Massnahmen zur Risiko-Steuerung eine enorme Bedeutung zu. Diese ist ein wesentlicher Bestandteil des Unternehmens-Risiko-Managements und muss mit viel Fingerspitzengefühl angegangen werden. Das Risiko-Management basiert auf der Risk Policy, die der Verwaltungsrat verabschiedeten hat. Sie legt die Leitlinien des Risiko-Managements für das Unternehmen schriftlich fest.

Durch die digitale Transformation wird die Risikosituation von Unternehmen noch komplexer, denn das Partner-/Lieferantennetzwerk wird immer umfangreicher und die Anzahl Anwendungen und Schnittstellen wächst ständig. Das ist eine umfangreiche Aufgabe, die es zu managen gilt!

Cyberrisiken haben sich deshalb in den letzten Jahren zu den grössten operativen Risiken für Unternehmen entwickelt. Dabei gilt es u.a. unternehmenskritische Elemente der IT-Infrastruktur vor Ausfall, Fehlfunktionen oder Manipulation zu schützen. Klassische IT-Sicherheit ist dabei aber nur ein Teil und umfasst dabei lediglich den Schutz Ihrer Systeme. Dieser ist zweifelsohne notwendig, aber heutzutage nicht mehr ausreichend. Entscheidend ist die Widerstandsfähigkeit des gesamten Unternehmens – sprich, dass die Prozesse, Mitarbeitenden und die IT-Infrastruktur auf interne und externe Risiken vorbereitet sind und Ihr Unternehmen im Ereignisfall schnell reagieren kann. Dies verstehen wir unter Cyber Resilience – und Sie sind in Ihrem Unternehmen dafür verantwortlich.

2 SO BEKOMMEN SIE IHRE CYBERRISIKEN IN DEN GRIFF

Was bedeutet das nun konkret für Sie als Entscheidungsträger? Es ist wichtig, dass Sie eine Übersicht über die tatsächlichen Cyberrisiken haben, denen Ihr Unternehmen Tag für Tag ausgesetzt ist. Nur wenn die Risiken bekannt und verstanden werden, können die Investitionen in die Cyber Security effizient gesteuert werden. Aus unserer Sicht, sind dies die wichtigsten Aspekte:

- Cyber Resilience auf oberster Unternehmensebene wahrnehmen
- Entwicklung konkreter Risikoszenarien
- Definition von Risikobehandlungs-Strategien
- Aufbau eines unternehmensweiten Cyber Risk Managements Teams
- Berücksichtigung aller beteiligten Parteien, wie Lieferanten, Partner, usw.
- Kontinuierliches Cyber Risk Monitoring

Das Cyber-Risikomanagement bildet die Basis und dient dazu, Gefahren und Risiken frühzeitig zu erkennen, zu behandeln sowie proaktiv Aktionen und Massnahmen für den Ereignisfall zu definieren. Dabei empfehlen wir Standards und Best Practices als Orientierungshilfe zu nutzen. Die Version 1.1 des NIST Cyber Security Frameworks sowie der IKT-Minimalstandard tragen den neuen technologischen Entwicklungen Rechnung und bieten ein anerkanntes Framework für das Cyber-Risikomanagement. Hilfreiche Ansatzpunkte liefern Ihnen auch die Normen ISO/IEC 31000 (Risikomanagement) und ISO/IEC 27005 (Information Security Risk Management). Nutzen Sie diese beim Aufbau Ihres unternehmensweiten Cyber Risk Managements.

2.1 Nehmen Sie Cyber Resilience auf oberster Unternehmensebene wahr

«Gute Manager managen Risiken, schlechte Manager managen Probleme!» Gerade in einer Zeit mit tiefgreifenden Veränderungen kommt dieser Aussage eine zentrale Bedeutung zu. Durch vorausschauendes Handeln können Risiken identifiziert, effizient gemanagt und damit Probleme, resp. Gefahren von vornherein vermieden werden.

Der Verwaltungsrat trägt die Verantwortung für die Identifikation, Einschätzung, Steuerung und Überwachung von Cyberrisiken und der entsprechenden Widerstandsfähigkeit. Er kann die Handlungsverantwortung selber übernehmen oder diese an ein bereits bestehendes Gremium (z.B. Prüfungsausschuss oder Risikoausschuss) oder an ein spezifisches Cyber Resilience-Gremium delegieren. Die Führungsverantwortung kann jedoch nicht delegiert werden. So oder so gilt es, den Umfang und die Zuständigkeiten sowie die Art und Weise, in der diese Zuständigkeiten wahrgenommen werden sollten, schriftlich festzulegen – einschliesslich der Struktur und Prozesse zur Überprüfung der Cyber Resilience.

Als Führungskraft müssen Sie sicherstellen, dass das Management Ihre Cyber Resilience und die Cyber-Risikobewertung in die allgemeine Geschäftsstrategie und das unternehmensweite Risikomanagement sowie die Budgetierung und Ressourcenallokation integriert wird.

2.2 Entwickeln Sie Risikoszenarien und definieren Sie den Umgang mit Risiken

Sie als Mitglied der Geschäftsleitung tragen die Verantwortung für die Risiko-Berichterstattung mit einer quantifizierten und nachvollziehbaren Bewertung von Cyberrisiken, Bedrohungen und Ereignissen. Sie validieren diese Bewertungen mit einer strategischen Risikobewertung unter Verwendung eines Risikomanagement-Frameworks. Das Ziel des Frameworks ist es, den identifizierten Risiken verantwortliche Personen/Rollen zuzuweisen. Diese müssen die Risiken überwachen (Monitoring), beurteilen und adäquate Massnahmen umsetzen, um die Risiken innerhalb der vorgängig definierten akzeptablen Grenzen zu halten (Risikoappetit).

Denken Sie dabei aber immer daran: Nicht alle Mitglieder des Managements sind Cyber Security Experten. Dank dem Einsatz von Werkzeugen zur Sicherheitsbewertung lassen sich technische Cybersicherheitsprobleme in eine leicht verständliche Sprache übersetzen. So ist Ihr Unternehmen besser in der Lage, Risiken ans Licht zu bringen und schneller zu beheben.

Für die adressatengerechte Kommunikation der Risiken empfiehlt es sich, Szenarien zu skizzieren. Diese Risiko-Szenarien helfen, die tatsächlichen Auswirkungen von Risiken auf das Unternehmen und dessen Stakeholder sichtbar und besser verständlich zu machen – auch ohne vertiefte Cyber Security-Kenntnisse. Dies hilft bei der Entscheidung, ob die Risiken aktiv behandelt werden sollen oder die Risiken gemanaged werden können. Die Reaktion auf die Risiken erfolgt dann nach einem strukturierten Ansatz. Idealerweise berücksichtigt dieser die Kritikalität des Risikos sowie den Aufwand zur Umsetzung von Massnahmen zur Risikobehandlung.

Sind die Risiken bekannt und die Strategie zum Umgang definiert, gilt es, diese kontinuierlich zu überwachen. Änderungen im Umfeld der Unternehmung können sich direkt auf die Risikosituation auswirken. Dies kann einerseits dazu führen, dass bekannte Risiken wichtiger oder weniger wichtig werden. Aber auch, dass neue Risiken hinzukommen, die bis anhin noch nicht bekannt waren.

2.3 Aufbau eines interdisziplinären Cyber Risk Management Teams

Der Aufbau eines effizienten Cyber Risk Management-Programms in einem Unternehmen setzt gewisse Strukturen voraus. Unabhängig vom ausgewählten Risiko-Management Framework setzt sich ein solches Programm meist aus der Identifikation, der Beurteilung, der Behandlung und dem Monitoring von Risiken zusammen.

Die Interdisziplinarität im Risk Management-Team ist hierbei ein wichtiger Faktor. So ist es beispielsweise unabdingbar, Spezialisten aus den Fachbereichen zu involvieren. Nur so können Sie verstehen, welche Kritikalität die verarbeiteten Daten haben. Denn der Bezug von Outsourcing-Leistungen wie Cloud-Diensten und ähnlichen läuft in Unternehmen meist über einen zentralen Einkauf. So erlangt man eine gute Übersicht über eine mögliche Konzentration von Anbieter- oder Third Party-Risiken.

2.4 Beziehen Sie auch Drittparteien in Ihre Risikobetrachtung mit ein

Um eine systemische Cyber Resilience zu gewährleisten, empfehlen wir Ihnen auch Drittparteien wie Partner-/Lieferanten in die Cyber-Risikobetrachtung einzubeziehen – soweit dies relevant und angemessen ist. Das Drittparteien-Management ist dabei ein wichtiger Schritt und befasst sich mit der Identifizierung sowie der Verwaltung von Cyberrisiken zu externen Drittparteien (d.h. Partner, Dienstleistern, Lieferanten von Hard- und Software, Outsourcing-Anbietern, Cloud-Service-Anbietern etc.). Durch die Implementierung von Anforderungen an die Cyber Security in formale Verträge, sollen die Risiken gezielt bewirtschaftet werden.

Deshalb hat das Lieferantenmanagement (Supply Chain Management) in den vergangenen Jahren immer mehr an Bedeutung gewonnen – insbesondere in Bezug auf die Berücksichtigung von Aspekten der Informationssicherheit.

Wir sind uns bewusst, dass der Umgang von Cyber-Sicherheitsrisiken innerhalb der Lieferanten- und Partnernetzwerke eine grosse Herausforderung ist. Gerade deshalb sollten Sie bestehende Standards, Best Practices und unterstützende Werkzeuge nutzen. So beschreibt beispielsweise ISO/IEC 27036:2013[1] die Informationssicherheit für Lieferantenbeziehungen. Auch das NIST CSF (v1.1)[2], der IKT Minimalstandard[3] und ISO/IEC 27001:2013[4] berücksichtigen «Supply Chain Risk Management», um Prozesse zur Erkennung, Bewertung und Steuerung von Risiken in der Lieferantenkette einzurichten.

Dabei geht es um eine bewusste Ausweitung des eigenen Risikomanagements und der Cyber Security auf die Lieferanten. Die Vorteile liegen auf der Hand: Nur so ist es möglich, die erforderliche Transparenz über die Cyberrisiken und die Maturität bezüglich Cyber Security innerhalb der Lieferkette zu erhalten.

[1] https://www.iso.org/standard/59688.html
[2] https://www.nist.gov/cyberframework/framework
[3] https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html
[4] https://www.iso.org/standard/54534.html

2.5 Überprüfen Sie Ihre Cyber Resilience regelmässig

Ein wichtiger Schwerpunkt liegt unbestritten in der Erkennung von Risiken. Die Kommunikation und Überprüfung von Cyber-Sicherheitsanforderungen zwischen Ihrem Unternehmen und beteiligten Drittparteien ist ein weiterer Aspekt. Hierbei muss sichergestellt sein, Daten und digitales geistiges Eigentum zu schützen, wie es die eigenen Cyber Security-Anforderungen verlangen.

Im Bedarfsfall kann dies mittels Security Assessments, Schwachstellen-Scans oder Penetration Tests verifiziert werden. Professionelle Lösungen helfen Ihnen das Cyber Risk Management ressourceneffizient umzusetzen. Die Vorteile liegen auf der Hand: Nur mit solchen Lösungen ist es möglich, die erforderliche Transparenz über Ihre Cyberrisiken zu erhalten, diese zu managen und nachhaltig zu minimieren.

Stellen Sie sicher, dass jährlich eine formelle, unabhängige Überprüfung (sofern sinnvoll und angemessen) der Cyber Resilience Ihres Unternehmens durchgeführt wird. Ebenfalls ist es Ihre Aufgabe dafür zu sorgen, dass die Erkenntnisse daraus in den kontinuierlichen Verbesserungsprozess einfliessen.

2.6 Cyber Risk Monitoring als wichtiger Bestandteil des Cyber Risk Managements

Wichtig ist, dass die Risikoanalyse permanent auf Aktualität und Stimmigkeit hin überprüft wird. Jeder, der unternehmerisch tätig ist, weiss, dass die Wirtschaft sich ständig verändert und Firmen auf die veränderten Rahmenbedingungen reagieren müssen. Hinzu kommt, dass sich im Laufe der Zeit auch die Risikotoleranz eines Unternehmens verändern kann. Die Stufen der Rahmenparameter, die Schadensdefinitionen, die Risikobewertungen und die Handlungsanweisungen sollten daher konsequent und fortlaufend validiert werden. Deshalb ist nicht nur eine einmalige Risikobewertung wichtig, sondern es muss eine regelmässige Überwachung stattfinden und eine Risikostrategie festgelegt werden (reduzieren, akzeptieren, auslagern etc.), um schliesslich einem «Leading Practice-Ansatz» gerecht zu werden.

Cyberrisiken sind nicht statisch

Es ist deshalb unerlässlich, jederzeit die Cyberrisiken im Auge zu behalten. Cyberrisiken sind keine statischen Gegebenheiten, sondern ein sehr dynamisches Objekt – und dieses muss regelmässig beobachtet werden:

- **Rahmenbedingungen ändern sich**
  Die heutige Businesswelt ist extrem dynamisch und so wirken von aussen immer neue Einflüsse auf Ihr Unternehmen ein, die beachtet werden müssen. Die initiale Cyberrisikoanalyse wird unter bestimmten Voraussetzungen durchgeführt. Ändern sich diese, so müssen zwangsläufig auch die Risiken neu bewertet werden.

- **Eintrittswahrscheinlichkeiten ändern sich**
  Eine initiale Risikoanalyse basiert auf den zu dem Zeitpunkt vorliegenden Informationen. Wie wir ausgeführt haben, können sich diese jederzeit ändern. Ein Cyberrisiko, das ursprünglich als sehr unwahrscheinlich angesehen wurde, kann plötzlich eine höhere Priorität erhalten. Ebenso kann der umgekehrte Fall eintreten. Wenn sich Eintrittswahrscheinlichkeiten verschieben, kann sich das wiederum auf die geplanten Massnahmen und die Planung auswirken.

- **Umsetzung der Massnahmen müssen überwacht werden**
  Wenn Sie aus der initialen Risikoanalyse Massnahmen abgeleitet haben, um die Cyberrisiken zu minimieren, ist das sehr gut! Leider erledigen sich diese nicht von selbst. Zum Cyber Risk Monitoring gehört also auch die Überprüfung, ob die Massnahmen effektiv umgesetzt wurden. Insbesondere wenn die Verantwortung für die Umsetzung an weitere Personen delegiert wurde, schadet es nicht, den Fortschritt zu überprüfen.

- **Auswirkungen von Massnahmen müssen überwacht werden**
  Selbst wenn alle Massnahmen wie geplant umgesetzt wurden, heisst das noch lange nicht, dass die Cyberrisiken damit auch tatsächlich minimiert wurden. Was ist, wenn die Massnahmen nicht wie geplant wirken? Oder vielleicht gar nicht mehr den aktuellen Gegebenheiten entsprechen? Im Rahmen des Cyber Risk Monitorings sollte auch geprüft werden, ob die Wirkung der Massnahmen den Erwartungen entsprechen.

Cyber Risk Management und das entsprechende Monitoring sind aus diesem Grund wichtige Aspekte im ganzen Sicherheitsdispositiv eines Unternehmens und eines Unternehmens als vertrauenswürdiger Partner.

3 FAZIT

Cyberrisiken sind business-kritisch, da sind wir uns wohl alle einig. Sie stellen eine omnipräsente Bedrohung dar und beeinflussen alle beteiligten Parteien – das eigene Unternehmen selbst, Kunden und Partner. Wenn es bei Ihnen, einem Lieferanten oder Partner zu einem Sicherheitsvorfall kommt, können die Auswirkungen auf die eigenen Prozesse und/oder die Prozesse vor- oder nachgelagerter Partner in der Wertschöpfungskette schwerwiegend sein. Aber auch ohne die Abhängigkeit von Dritten unterliegt Ihr Unternehmen zunehmenden Cyberrisiken – und immer mehr sind Schweizer Unternehmen im Fokus von Cyberkriminellen.

Die Sicht auf die eigenen essentiellen Cyberrisiken stellt viele Unternehmen vor eine grosse Herausforderung. Die zunehmende Dynamik und die sich verändernde Einschätzung beeinflusst die Risikoexposition Ihres Unternehmens erheblich. Die Herausforderungen bei der Bewältigung von Cyber-Sicherheitsrisiken sind zahlreich. Wesentliche Schwierigkeiten basieren unserer Erfahrung nach auf:

- den fehlenden Ressourcen und/oder Tools;
- den Herausforderungen bei der systematischen Bewertung und Überwachung der Risiken, was hauptsächlich auf mangelnde Transparenz und Schwierigkeiten bei der Identifizierung von Abhängigkeiten zurückzuführen ist;
- der grossen Anzahl der beteiligten Personen und Drittparteien;
- den organisatorischen Herausforderungen bei der Umsetzung und Kontrolle von Cyber Security-Vorgaben.

Diese Schwierigkeiten zeigen leider, dass das Cyber-Risikomanagement heute noch immer ein vernachlässigtes Thema darstellt. Dabei sind gerade Cyberrisiken elementar und dürfen nicht ausser Acht gelassen werden. Verschaffen Sie sich Klarheit über Ihre Cyberrisiken – und ziehen Sie bei Bedarf externe Experten zu Hilfe.

Danke, dass Sie sich Zeit genommen haben für unser
«Cyber Risk Management Whitepaper».

Ihre InfoGuard

4 IHR PARTNER FÜR CYBER SECURITY & CYBER RISK MANAGEMENT

InfoGuard ist der Schweizer Experte für umfassende Cyber Security. Profitieren auch Sie von unserer Erfahrung, Professionalität und Zuverlässigkeit in Audit, Beratung, Architektur und Integration führender Security-, Netzwerk- und Cloud-Lösungen. Innovative Managed und Cyber Defence Services erbringen wir aus unserem InfoGuard Cyber Defence Center in der Schweiz. Unsere über 150 Sicherheitsspezialisten in Zug und Bern sorgen täglich für die Informationssicherheit bei über 300 Kunden in der Schweiz.

SECURITY CONSULTING SERVICES

Risiken erkennen und beherrschen

Ob Cyber Security, Cyber Risk Resilience, Governance, Risk & Compliance, Digitalisierung oder Cloud: Die wachsenden Herausforderungen lassen sich nur mit einer ganzheitlichen Cyber Security-Strategie meistern. Das modular aufgebaute Dienstleistungsangebot von InfoGuard berücksichtigt Technologien, Prozesse und Ihre Mitarbeitenden gleichermassen. Die langjährige Erfahrung im Bereich der Sicherheitsberatung nach ISO 27xxx und NIST, Penetration Testing, Attack Simulation sowie Security Awareness und die erstklassigen Kompetenzen unserer Spezialisten stellen das reibungslose Zusammenspiel aller Elemente sicher.

NETWORK & SECURITY SOLUTIONS

ICT-Infrastrukturen optimieren und schützen

Effiziente Netzwerk- und Security-Infrastrukturen müssen das Optimum aus Performance, Sicherheit und Kosten erreichen. Das gelingt nur, wenn alle Komponenten perfekt aufeinander abgestimmt sind. InfoGuard bietet ein vollständiges Portfolio führender Security-, Netzwerk- und Cloud-Lösungen für konventionelle, virtualisierte, containerisierte sowie Cloud-Infrastrukturen. Dafür arbeiten wir in jedem Teilgebiet mit den jeweils besten Herstellern zusammen. Unsere erfahrenen und zertifizierten Experten unterstützen Sie von der Architektur und dem Design über das Engineering und die Integration bis hin zum Betrieb On-premise, in der Cloud oder als Managed Service.

CYBER DEFENCE SERVICES

Cyberattacken erkennen und eliminieren

Unternehmen müssen heutzutage davon ausgehen, dass Cyberangriffe nicht nur stattfinden, sondern auch erfolgreich sind. Deshalb sind wirkungsvolle Abwehrmassnahmen kombiniert mit Services zur Erkennung und Bewältigung von Vorfällen immer wichtiger. In unserem ISO/IEC 27001:2013 zertifizierten und ISAE 3000 Typ 2 überprüften Cyber Defence Center in der Schweiz bündeln wir erstklassiges Fachwissen und hochentwickelte Technologien mit der langjährigen Erfahrung unserer Security-Experten und Threat-Analysten. Unsere umfassenden Cyber Defence Services schützen Ihre On-Premise-, Cloud-, IoT- und OT-Infrastrukturen rund um die Uhr.

InfoGuard AG
Lindenstrasse 10
6340 Baar / Schweiz
Tel +41 41 749 19 00
info@infoguard.ch

InfoGuard AG
Office Bern
Stauffacherstrasse 141
3014 Bern / Schweiz
Tel +41 31 556 19 00

INFOGUARD.CH