KPMG

Ein neues Konzept für die Cyber-sicherheit

Feel Free

kpmg.ch

DIE GRUNDSÄTZE UNSERES KONZEPTS

Wir sind der Meinung, dass beim Thema Cybersicherheit die Möglichkeiten im Mittelpunkt stehen sollten und nicht die Einschränkungen.

AN GESCHÄFTLICHEN ZIELEN ORIENTIERT

Wir arbeiten mit Ihnen zusammen, um Ihr Unternehmen voranzubringen. Der positive Umgang mit Cyberrisiken hilft Ihnen nicht nur, die Unsicherheit in Ihrem Geschäftsbetrieb unter Kontrolle zu bringen. Sie können daraus einen echten strategischen Vorteil machen.

KLARE ERKENNTNISSE

Die rasante Digitalisierung mit immer neuen Bedrohungen und Möglichkeiten erfordert flexibles Handeln und einen sicheren Rückhalt. Unsere Experten kennen sich sowohl bei der Cybersicherheit als auch in Ihrem Markt bestens aus. So vermitteln wir Ihnen wertvolle Erkenntnisse, überzeugende Ideen und bewährte Lösungen, damit Sie fundiert agieren können.

SEITE AN SEITE

Wir arbeiten mit Ihnen als langfristige Partner zusammen und bieten Ihnen die Beratung und Herausforderung, die Sie brauchen, um fundiert zu entscheiden. Wir wissen, dass dieser Bereich oft durch Gefühle des Zweifels und der Gefährdung überschattet wird. Deshalb arbeiten wir Hand in Hand mit Ihnen, geben Ihnen ein echtes Gefühl von Sicherheit und eröffnen Ihnen damit Handlungsspielräume.

FEEL FREE

Ein positives Konzept für den Umgang mit Cyberrisiken kann Freiräume eröffnen

CYBERSICHERHEIT VERSTEHEN

Die Digitalisierung bietet viele Chancen für Unternehmen, die neue Märkte erobern wollen und bereit sind, in tiefgreifende Veränderungen zu investieren. Seit zehn Jahren erleben wir eine rasante Ausbreitung neuer Technologien, eine verstärkte Vernetzung von Unternehmen und Privatpersonen und einen Welthandel, der rund um die Uhr läuft. Vielen Unternehmen fällt es jedoch schwer, mit dieser Entwicklung Schritt zu halten und ihre geschäftlichen Ziele zu erreichen, ohne sich durch Cyberrisiken bedroht zu fühlen.

Tag für Tag erfahren wir von neuen Sicherheitslücken, Angriffen und Zwischenfällen. Ein Bericht[1] des renommierten Thinktanks *The Centre for Strategic and International Studies* bezifferte die dadurch entstehenden Verluste kürzlich auf USD 375–575 Milliarden und mutmaßte, dass die Cyberkriminalität durch Betrug und Spionage Kosten von bis zu 20 % der weltwirtschaftlichen Wertschöpfung durch das Internet verursachen könnte.

Da sich die Bedrohungslandschaft ständig weiterentwickelt, sind Cyberrisiken in der Wirtschaft ein alltägliches Thema. Daraus ergibt sich ein Gefühl der Gefährdung, das von manchen genutzt wird, um höhere Budgets durchzusetzen und Produkte zu verkaufen. Wir stellen oft fest, dass dies zu hohen Investitionen in wirkungslose Programme führt, die zudem schlecht auf die jeweiligen Risiken und geschäftlichen Notwendigkeiten abgestimmt sind. Cybersicherheit ist keine technische Sofortlösung und auch kein Thema, das allein die IT-Abteilung betrifft.

Wir bei KPMG erleben allzu oft, dass die Unternehmensführung aufgrund dieser Verhaltensweisen nicht weiß, was sie eigentlich tun muss, welcher Aufwand angemessen ist und auf wessen Hilfe sie sich verlassen kann, um auf der sicheren Seite zu sein.

Wir glauben, dass ein positives Konzept für den Umgang mit Cyberrisiken, das traditionelle Denkweisen auf den Kopf stellt, Unternehmen Freiräume eröffnet, die ihnen helfen, ihre geschäftlichen Ziele zu erreichen.

[1] Net Losses: Estimating the Global Cost of Cybercrime, Juni 2014

RUNDUMBLICK AUF DAS THEMA CYBERSICHERHEIT

ANGSTFREI AGIEREN

Panikmache ist immer einfach. Wer jedoch auf dem Laufenden bleibt und weiß, wie sich die Bedrohungslandschaft entwickelt und wie sie sich auf ihn auswirkt, kann Angst, Unsicherheit und Zweifel ausräumen.

Es ist wichtig, die Bedrohungen von außen durch Hacktivisten, organisierte Kriminalität, Industriespionage und zunehmend auch durch Nationalstaaten zu verstehen. Allzu leicht vergisst man jedoch die Bedrohungen von innen, die von unachtsamen, verärgerten oder böswilligen Mitarbeitenden ausgehen. Oft verschaffen sich Angreifer durch Phishing-E-Mails und andere Social-Engineering-Angriffe Zugang zu Mitarbeiterkonten. Auch Bestechung und Einschüchterung sind in den meisten Teilen der Welt noch immer an der Tagesordnung. Wenn Bedrohungen von außen und von innen nicht isoliert, sondern gemeinsam angegangen werden, entsteht ein integriertes Konzept, das die Angst und Unsicherheit in Bezug auf die Herkunft von Angriffen ausräumt.

Viele Angreifer nutzen einfach nur andere Mittel, um ein sehr altes Ziel zu erreichen – sei es Diebstahl, Subversion, Sabotage oder Spionage. Wer Parallelen zwischen der Sicherheit in der realen und der virtuellen Welt zieht, kann der Angst vor dem Unbekannten den Boden entziehen.

Wir von KPMG analysieren Motivation und Absichten des Angreifers sowohl in der realen als auch in der virtuellen Welt und folgern daraus, wie er Ihre Systeme gefährden könnte. Anhand dieser Erkenntnis können wir Ihre Schwachstellen aufdecken und Sie bei der Einrichtung ihrer Abwehrmechanismen beraten.

Wenn Sie flexibel sind und mit Veränderungen und Verwerfungen rechnen, können Sie eine Umgebung planen, die von Grund auf sicher ist.

EINE UNABHÄNGIGE MASSGESCHNEIDERTE BERATUNG KANN IHNEN DAS NÖTIGE VERTRAUEN VERMITTELN, UM IHRE WACHSTUMSZIELE ZU VERFOLGEN

Zunächst müssen Sie die richtigen Grundlagen in Bezug auf Governance, Risiko und Compliance schaffen. Anschließend können Sie einen Ausgleich zwischen technischer Sicherheit, internen Fähigkeiten und dem angemessenen Einsatz von Technologie und ausgelagerten Dienstleistungen schaffen.

Wir glauben, dass der Erfolg den Unternehmen gehört, die die Beherrschung von Cyberrisiken in sämtliche Aktivitäten integrieren.
Wer fundierten Grundsätzen folgt und keine Veränderungen scheut, statt nur von Fall zu Fall auf Probleme zu reagieren, kann ein umfassendes Konzept erstellen, in dessen Mittelpunkt die Möglichkeiten stehen und nicht die Einschränkungen.

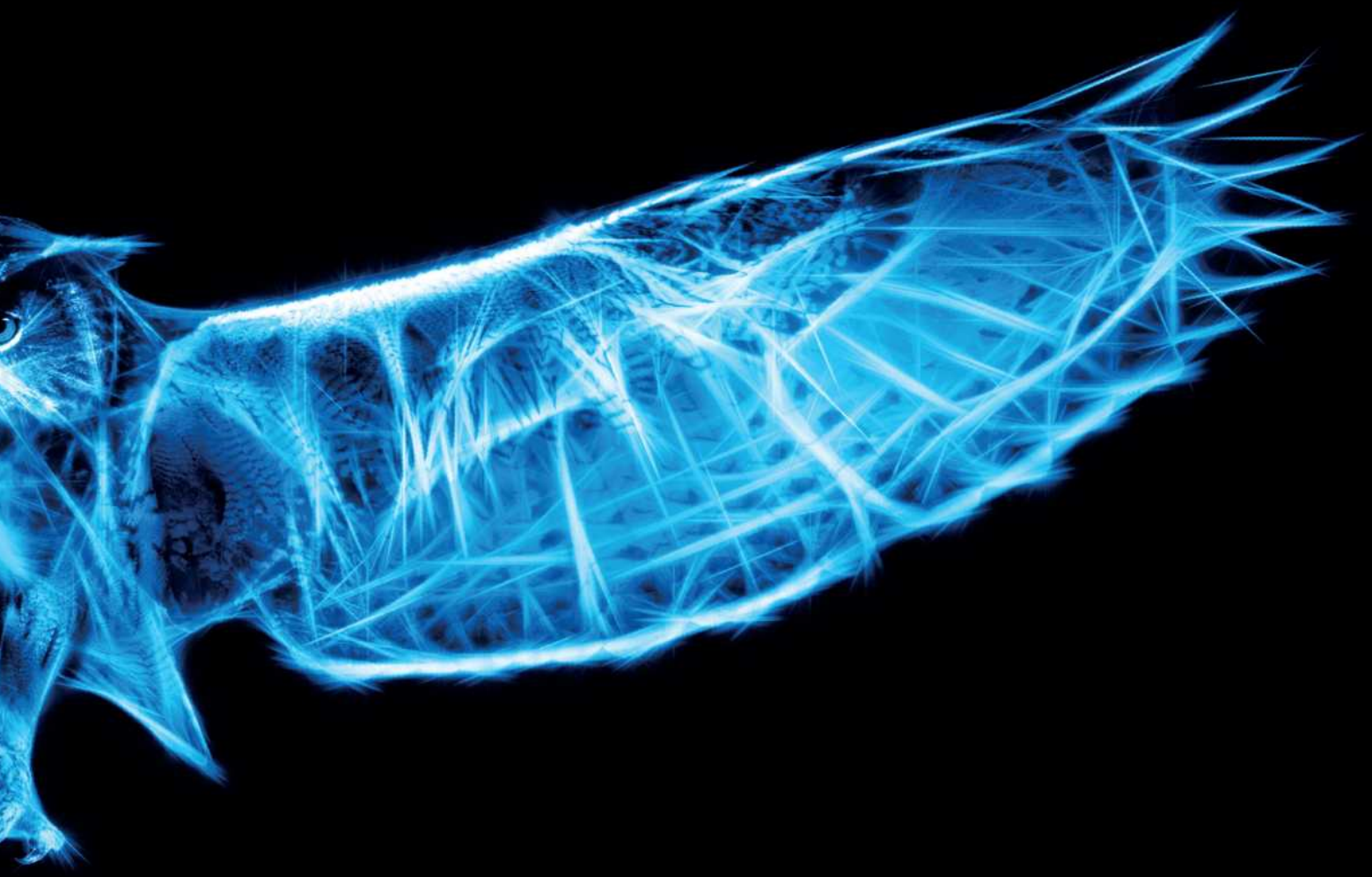
FREIRÄUME FÜR HERAUSFORDERUNGEN

Die britische Regierung setzt regelmäßig Initiativen zur Sensibilisierung für Cyberbedrohungen um. Verwaltungsräte müssen ihre Teams herausfordern, um Antworten auf die richtigen Fragen zu erhalten, bevor ihre eigene Kompetenz und Kontrolle von den Stakeholdern in Frage gestellt wird. Die Fähigkeit, den Informationslebenszyklus zu identifizieren, zu priorisieren und zu schützen, hilft Ihnen, sicher zu agieren.

Wir von KPMG können Ihnen helfen, Ihre Abhängigkeiten in der Lieferkette zu verstehen, mit Ihrer Gemeinschaft zusammenzuarbeiten, um Cyberrisiken zu verstehen, Informationen über Bedrohungen weiterzugeben und die Bereitschaft zu gemeinsamen Reaktionen zu verbessern.

Wenn Sie über eine robuste Strategie und Architektur verfügen, haben Sie Zugang zu klaren und umsetzbaren Managementinformationen, auf die Sie sich bei Ihren Entscheidungen stützen können. Außerdem haben Sie Zugriff auf Erkenntnisse über aktuelle Bedrohungen, verlässliche Netzwerke für den Informationsaustausch und glaubwürdige Benchmark-Vergleiche mit Konkurrenten. Informationsquellen müssen objektiv und von den Interessen einzelner Anbieter unabhängig sein. Wenn Sie Zugriff auf verlässliche Quellen haben, können Sie die richtige Mischung aus Technologie, Dienstleistern und internen Fähigkeiten testen und prüfen, um Kontrolle mit Transparenz zu verbinden.

Wir glauben, dass Kooperation und Wissen an dieser Stelle einen echten geschäftlichen Vorteil bringen. Wenn Sie die geballte Erfahrung von Menschen nutzen, denen Sie vertrauen, haben Sie die nötige Sicherheit, um neue Ideen, Konzepte und Lösungen umzusetzen, mit denen Sie den Sicherheitsproblemen von heute und morgen begegnen können.



FREIRÄUME FÜR HÖHENFLÜGE

FREIRÄUME FÜR INVESTITIONEN

Mit jedem Aspekt einer neuen Technologie stellen sich neue Überlegungen – von der Einführung von Cloud-Technologien über die Ausbreitung sozialer Medien bis zur Telearbeit. Mit einem effizienten Management sind dies Investitionsmöglichkeiten, die ein hohes Wachstumspotenzial bieten.

Auch der Vormarsch der Mobiltechnologie und ihrer Anwendungen berührt alle Branchen und Geschäftsmodelle. Unternehmen müssen im Zusammenhang mit diesen neuen Technologien Entscheidungen treffen und im Voraus verstehen, welche Probleme sich für die Cybersicherheit ergeben. Nur so lässt sich das richtige Gleichgewicht zwischen Risiken und Chancen finden.

Wir von KPMG ermitteln gemeinsam mit Ihnen den Investitionsbedarf, damit Ihnen die Beherrschung von Cyberrisiken Freiräume eröffnet, die Ihnen die Erreichung Ihrer geschäftlichen Ziele ermöglichen.

Eine unabhängige und maßgeschneiderte Beratung hinsichtlich der Frage, welche Sicherheitsdienste, -technologien und -konzepte zu Ihrer Kultur passen, kann Ihnen die nötige Sicherheit geben, um Ihre Wachstumsziele zu verfolgen.
Wir können Ihnen helfen, Ihre konkrete Bedrohungslage, die für Ihr Geschäft maßgebliche Regulierungslandschaft und Ihre eigenen Anlagen umfassend zu verstehen.

Wir glauben, dass Investitionen in ein proaktives Konzept für den Umgang mit Cyberrisiken grundsätzliche wirtschaftliche Vorteile bieten. Hier geht es um die Sicherheit, dass Ihr Unternehmen im Zuge der unaufhaltsamen Digitalisierung gezielt und flexibel wachsen kann.

DIE BEHERRSCHUNG VON CYBERRISIKEN ERÖFFNET FREIRÄUME

FREIRÄUME FÜR VERÄNDERUNGEN

Momentan werden viele Unternehmen nur bei schweren Sicherheitsverletzungen aktiv. Mit einer proaktiven Einstellung zum Thema Sicherheit lassen sich Angreifer ausbremsen und ihre Handlungen frühzeitig erkennen. Die Entwicklung eines anpassungsfähigen Konzepts kann verhindern, dass es zu Ausfallzeiten kommt, teure und störende Reaktionen auf Zwischenfälle erforderlich werden und der Geschäftsbetrieb unterbrochen wird. Wenn Sie die Szenarien für Cyberangriffe und die sich wandelnde Bedrohungslandschaft durchdenken, werden Sie besser verstehen, wie Ihr Unternehmen ins Visier genommen werden könnte und wie Sie Ihre Abwehr einrichten müssen.

Wir von KPMG legen bei unserem Konzept großen Wert darauf, die knappen Ressourcen eines Unternehmens optimal zu nutzen. Wir beginnen zunächst mit einem von Grund auf sicheren Konzept, bei dem zur Verstärkung der Wirkung frühzeitig in den Entwicklungslebenszyklus investiert wird.

Mit einem soliden Fundament können Sie Ihre Sicherheitsaktivitäten durch Führungskompetenz, Sponsorship und Governance untermauern. Dies hilft, die Bedingungen für die richtige Kultur festzulegen – eine Kultur, in der jedem Einzelnen bewusst ist, dass Sicherheit alle angeht und welche Rolle er selbst spielen kann und muss.

Wer die nötige Sicherheit für eine solche Veränderung hat, schafft die Integration von Strategie, Politik, Governance, Organisation, Prozess, Fähigkeiten und Technologie.

Wir glauben, dass Unternehmen, die Cyberangriffe als unvermeidlichen Bestandteil der heutigen Wirtschaft akzeptieren und die proaktive Sicherheitsmechanismen und Reaktionen einbauen, gut für die Zukunft gerüstet sind.

SICHERHEIT GEHT ALLE AN

WIR SIND ...

PREISGEKRÖNT

Ob im SC Magazine oder bei den MCA Awards: KPMG schneidet bei unabhängigen Preisen glänzend ab. Forrester würdigt KPMG auch als führendes Beratungsunternehmen in Sachen Informationssicherheit und verweist auf unsere starke Fokussierung und unsere Fähigkeit, anspruchsvolle Mandate zu übernehmen.

UNABHÄNGIG

Wir sind an keinen Technologie- oder Softwareanbieter gebunden. Alle unsere Empfehlungen und technischen Strategien basieren allein darauf, was für Ihr Unternehmen am besten geeignet ist.

GLOBAL UND LOKAL

Im KPMG-Firmennetzwerk arbeiten über 2000 Sicherheitsexperten. Dadurch können wir die benötigten Kompetenzen bündeln und weltweit stets hohe Ansprüche erfüllen. KPMG-Mitgliedsfirmen können Ihre lokalen Bedürfnisse erfüllen – von Strategie- und Veränderungsprogrammen im Bereich Informationssicherheit über technische Bewertungen, forensische Untersuchungen, Krisenbewältigung und Schulungen bis hin zur Zertifizierung nach ISO 27001.

KOOPERATIV

Wir organisieren und nutzen Kooperationsforen, um die besten Köpfe der Branche zusammenzubringen und zusammen mit ihnen gemeinsame Herausforderungen zu bewältigen. Das Forum I-4 von KPMG bringt über 50 der weltweit größten Unternehmen zu Gesprächen über neue Probleme und Lösungen zusammen.

VERTRAUENSWÜRDIG

Wir haben eine lange Liste von Zertifizierungen und Bewilligungen zur Arbeit bei führenden Unternehmen aus aller Welt.

DIE DIGITALISIERUNG BIETET VIELE CHANCEN FÜR UNTERNEHMEN, DIE NEUE MÄRKTE EROBERN WOLLEN UND BEREIT SIND, IN TIEFGREIFENDE VERÄNDERUNGEN ZU INVESTIEREN

IHRE ANSPRECHPARTNER

KPMG AG
Badenerstrasse 172
Postfach
CH-8036 Zürich

kpmg.ch

Matthias Bossardt
Partner, Cyber Security
T: +41 58 249 36 98
E: mbossardt@kpmg.com