KPMG
cutting through complexity

SECURITY CONSULTING

Datenzugriff für Unbefugte verboten!

Schutz der Informations-systeme durch risikoorientierte Sicherheitskonzepte

Connected World
Smart Business

Wir müssen uns alle von der Vorstellung verabschieden, dass Angreifer wirksam aus Unternehmensnetzen herausgehalten werden können.

Uwe Bernd-Striebeck
Partner, Security Consulting

Inhalt

1 Cyberrisiken: Haben Sie die Zeichen der Zeit erkannt?

Die schubweise ans Tageslicht kommenden Informationen über Ausspähprogramme von Regierungen sowie immer neue Meldungen über erfolgreiche Angriffe auf Unternehmen zeigen selbst in ihrer Unvollständigkeit deutlich: Die Daten- und Informationssicherheit steht unter Beschuss.

Edward Snowdens Enthüllungen haben auch zu der ernüchternden Erkenntnis geführt, dass Datenströme technisch umfassend analysierbar sind. Unternehmen müssen darauf angemessen reagieren – zumal die Aufsichtsbehörden Transparenz fordern über aufgetretene Sicherheitsvorfälle sowie über Maßnahmen, die Unternehmen zur Risikovorsorge ergreifen.

> „[…] there's no question that the US is engaged in economic spying."
>
> Edward Snowden

Bis 2015 werden **80 %** aller erfolgreichen Angriffe durch Ausnutzen von bekannten Schwachstellen erfolgen.

Bei der Verteidigung gegen Cyberrisiken und fortgeschrittene Bedrohungen („advanced persistent threats“) müssen Unternehmen umdenken: Cloud-Technologien, Digitalisierung und Vernetzung sowie die Konvergenz von privater und beruflicher IT-Nutzung (Social Media, bring your own device) führen dazu, dass herkömmliche Methoden wie Firewalls und Intrusion Detection-Systeme allein keinen wirksamen Schutz mehr bieten. Es wird auf absehbare Zeit technisch nicht möglich sein, Angreifer gänzlich aus den Unternehmensnetzen zu verbannen. Kurzum: Höhere Stadtmauern und tiefere Burggräben machen Unternehmen nicht sicherer!

Was können Sie tun?

Schutzlos ausgeliefert sind Sie Cyberattacken dennoch nicht. Vielmehr gibt es drei grundlegende Voraussetzungen, um bestmöglichen Schutz zu erreichen:

- Reaktionsfähige Security-Organisation
- Prozesse, die eine nachvollziehbare Einschätzung aktueller Bedrohungen und Ableitung zielgerichteter Maßnahmen ermöglichen, sowie
- Techniken und Produkte, die einerseits präventiv für den Basisschutz sorgen und andererseits durch aktives Monitoring Auffälligkeiten in der IT-Landschaft des Unternehmens identifizieren.

Das erfolgreiche Zusammenspiel von Organisation, Prozessen und Technik gewinnt an Bedeutung. Schließlich drohen Reputationsschäden durch Datenverlust, Schadensersatzansprüche bei fahrlässigem Umgang mit Daten oder auch Betriebsunterbrechungen bei Angriffen auf IT-Systeme. Und diese Themen sind keine Zukunftsmusik, sondern stehen bei vielen unserer Mandanten schon jetzt auf der Agenda. Auch die ersten Versicherer reagieren und richten die Höhe der Versicherungsprämien am Risikoprofil eines Unternehmens aus.

Unser Angebot

Unsere Dienstleistungen zum Schutz der Daten und Informationssysteme bündeln wir bei KPMG im Bereich Security Consulting. Dabei verfolgen wir einen ganzheitlichen Beratungsansatz. Zu unseren Leistungen gehören beispielsweise die Planung und Implementierung von Informationssicherheits-Managementsystemen (ISMS), technische Sicherheitsvorkehrungen, Identity & Access Management (IAM), Business Continuity Management (BCM), Design sicherer IT-Infrastrukturen sowie Penetrationstests zum Nachweis der Wirksamkeit installierter Abwehrmaßnahmen.

2 Sind die Unternehmen mit ihren Sicherheitsbemühungen am Ende?

Uwe Bernd-Striebeck verantwortet den Bereich „Security Consulting“ von KPMG in Deutschland. Im Interview kündigt der KPMG-Partner einen baldigen Paradigmenwechsel an, der die Wahrnehmung des Themas Informationssicherheit in den Unternehmen verändern wird.

Wie ist es um die IT-Sicherheit in deutschen Unternehmen bestellt?

Aus meiner Sicht: schlecht!

Wir müssen uns alle von der Vorstellung verabschieden, dass Angreifer wirksam aus Unternehmensnetzen herausgehalten werden können. Hier steht ein Paradigmenwechsel im Bereich der IT-Sicherheit an: In Zukunft wird es darum gehen, bereits im Netz befindliche Angreifer anhand von Anomalien zu erkennen und zu entfernen.

Und es besteht dringender Handlungsbedarf: Wir müssen neuartige Systeme einsetzen, die auf Anomalie-Erkennung spezialisiert sind. Tatsächlich hat heute kaum ein Unternehmen in Deutschland solche Systeme installiert. Eine funktionierende Anomalie-Erkennung ist für die meisten noch Zukunftsmusik. Aber unsere Security Audits zeigen auch, dass einige Unternehmen im Bereich der klassischen Sicherheitsmaßnahmen noch Nachholbedarf haben.

Zukünftig gilt: Absoluter Schutz nach außen gelingt den wenigsten Unternehmen – dies wäre unbezahlbar. Erfolgreiche Unternehmen investieren einerseits weiter in sinnvolle Abwehrmaßnahmen und erkennen andererseits im Fall der Fälle einen erfolgreichen Angriff frühzeitig. Nur durch die Kombination der Maßnahmen kann wirksam Schaden vom Unternehmen abgewendet werden.

Wo sehen Sie mittelfristig die größten Herausforderungen für Unternehmen?

Flächendeckende Informationssicherheit zu implementieren, wird in Zukunft unbezahlbar!

KPMG beschäftigt über **100 Mitarbeiter** im Bereich Security Consulting.

Für international tätige Unternehmen kommt es deshalb darauf an, streng risikoorientiert vorzugehen. Der Schutz der „Kronjuwelen" des Unternehmens muss oberste Priorität haben. Das spart auch Kosten. Für ihre sensiblen und geschäftskritischen Daten benötigen Unternehmen also maßgeschneiderte Schutzlösungen anstelle von standardisierten Sicherheitslösungen „out of the box".

Außerdem wird der regulatorische Druck auch im IT-Sicherheitsbereich weiter zunehmen. Themen wie ISO/IEC 27001-Zertifizierungen und Business Continuity-Vorgaben verlieren ihren optionalen Charakter und werden obligatorisch.

Sollten IT-Verantwortliche sich eher vor einem Angriff von außen fürchten oder werden die Risiken durch interne Datenverluste unterschätzt?

Bis jetzt waren Bedrohungen von innen das größere Problem: 30 bis 40 Prozent der IT-Sicherheitsverletzungen kamen aus dem eigenen Unternehmen. Dieses Verhältnis verändert sich gerade. Der Umfang der externen Wirtschaftsspionage nimmt stetig zu – aktuelle Medienberichte über Hackerangriffe auf namhafte Organisationen und Konzerne belegen dies deutlich. Mit „advanced persistent threats" (APT) steigt die Qualität der Angriffe deutlich – häufig richten sie sich heute sehr gezielt gegen ausgewählte Personen einer Gesellschaft.

So viel steht fest: Der Umgang mit aktuellen Bedrohungsszenarien muss sich ändern. Muss IT-Sicherheit zur Chefsache werden?

Ein deutliches „Ja"!

Nur ein ganzheitlicher Ansatz kann die Sicherheit der geschäftskritischen Informationen eines Unternehmens gewährleisten. Sicherheit muss als fester Bestandteil in allen wesentlichen Prozessen des Unternehmens fest verankert sein – und das ist Chefsache.

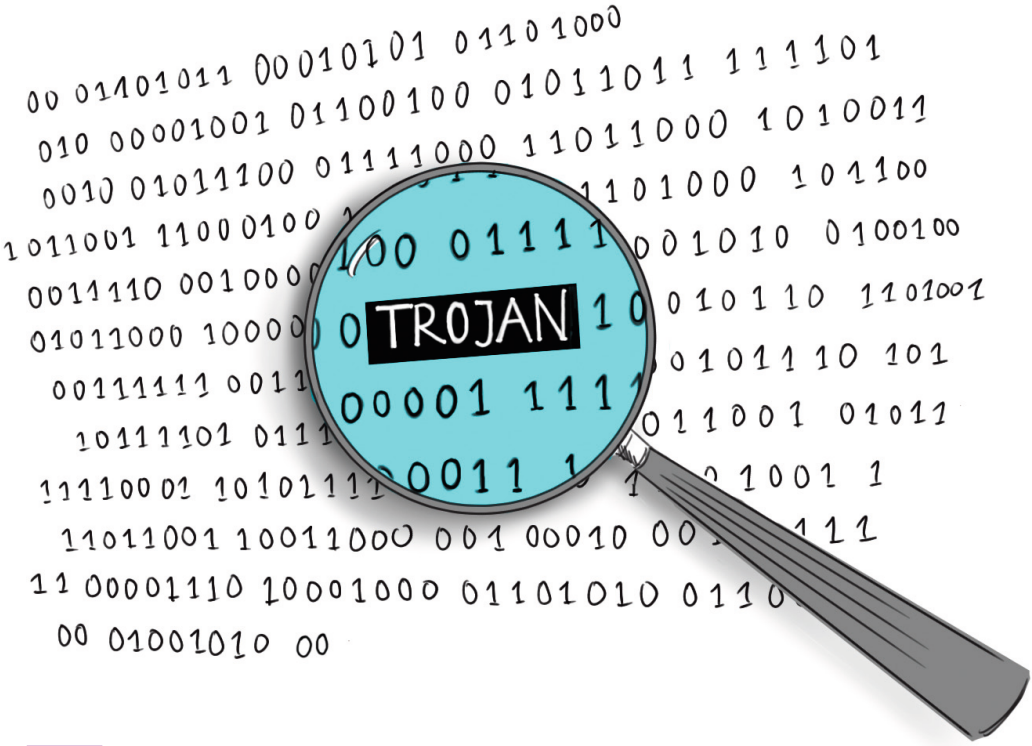
Allerdings beruht ein erfolgreiches Sicherheitsmanagement auch immer auf Teamwork: Unternehmen brauchen eine kompetente Mannschaft aus Entscheidungsträgern, die die Verantwortung für IT, Compliance, Sicherheit und Datenschutz übernehmen.

Daten: Welche sind wichtig, welche sind kritisch?

Durch Kosten- und Innovationsdruck sowie neue Markttrends gewinnt der Wettbewerbsfaktor Information rasant an Bedeutung. Häufig sind jedoch weniger als fünf Prozent der Daten im Unternehmen wirklich schützenswert.

> An Fortschritt glauben heißt nicht glauben, dass ein Fortschritt schon geschehen ist. Das wäre kein Glauben.
>
> Franz Kafka

Die Budgets für den Schutz von Informationen werden heute zu über 80 Prozent für präventive Technologien verwendet. Mit einem signifikanten Zuwachs in der personellen und finanziellen Ressourcenausstattung ist nicht zu rechnen. Eine moderne Security-Organisation muss sich deshalb zwei Herausforderungen stellen: Sie muss verstärkt risiko- und wertebasiert die sensibelsten beziehungsweise wichtigsten Informationen eines Unternehmens schützen. Allerdings können nicht alle Risiken präventiv angegangen werden. Daher sind ein ebenso zeitnahes wie transparentes Monitoring des Status quo und die Antizipation möglicher Angriffe unabdingbar. Und das wird nur gelingen, wenn wir uns von einigen alten, wenig effizienten Sicherheitsmaßnahmen verabschieden.



30 % der Unternehmen verzichten auf eine Risikoklassifizierung von Anwendungen und Systemen.

Was können Sie tun?

Unternehmen der gleichen Branche sind häufig auch vergleichbaren Bedrohungen ausgesetzt. Wettbewerber können deshalb im Bereich Security zu Partnern werden, um aus den Angriffsmustern zu lernen. So haben sich beispielsweise mehrere Handelsunternehmen zusammengeschlossen, um Identitätsdiebstähle im Internet nachzuvollziehen. Ein „Honigtopf" („honeypot") mit nahezu ungeschützten Login-Daten wurde dazu ins Netz gestellt. So konnte in der Folge die Zahl der Angreifer erfolgreich eingegrenzt werden. Vor diesem Hintergrund sollten Sie auch Ihre Sicherheit hinterfragen:

- Wissen Sie, wo in Ihrem Unternehmen die kritischsten Daten gespeichert werden?
- Können Sie ausschließen, dass kritische Daten auf privaten Rechnern Ihrer Mitarbeiter gespeichert sind?
- Haben Sie Sicherheitszonen zur Speicherung und Verarbeitung Ihrer IT-Systeme risikoorientiert implementiert?
- Wissen Sie, inwieweit die IT-Sicherheitsmaßnahmen in Ihrem Unternehmen bereits umgesetzt worden sind?
- Haben Sie über Expertengruppen oder Branchenverbände alle erforderlichen Informationen über Security-Bedrohungen Ihrer Branche oder der direkten Konkurrenz?

Unser Angebot

Der Schutz geschäftskritischer Informationen beginnt bei der Datenidentifikation und der Risikoanalyse. Auf dieser Basis können die Anforderungen an Vertraulichkeit, Integrität und Datenbeziehungsweise Systemverfügbarkeit definiert werden.

Gemeinsam mit Ihnen analysieren wir Ihre aktuelle Sicherheitsorganisation – damit Sie heute nicht in Schutzmaßnahmen investieren, die Ihnen morgen keinen Schutz mehr bieten.

Unser Leistungsangebot umfasst

- Prüfung Ihrer aktuellen Sicherheitskonzepte auf Angemessenheit
- Erfassung Ihrer kritischen Informationswerte
- Definition risikoorientierter Sicherheitskonzepte
- Aufbau von maßgeschneiderten Monitoring- und Reportingsystemen zum Status Ihrer Informationssicherheit.

4 Vorsorgen statt nachsehen: Kennen Sie Ihre Datenlecks?

> An allem Unfug, der passiert, sind nicht etwa nur die schuld, die ihn tun, sondern auch die, die ihn nicht verhindern.
>
> Erich Kästner

Unzählige Sicherheitsprüfungen und Penetrationstests in den letzten Jahren haben gezeigt, dass viele aktuelle Webauftritte und IT-Anwendungen ein hohes Risikopotenzial bergen. Über 80 Prozent der bisher von KPMG untersuchten Systeme wiesen gravierende Sicherheitslücken auf, die Datenmissbrauch und -diebstahl ermöglichen.

Die Bedrohung für Unternehmen sowohl aus dem Internet als auch aus den eigenen Reihen wächst. Dabei nimmt nicht nur die Anzahl der Attacken auf sensible Daten zu. Auch die Qualität und Zielstrebigkeit, mit der Angreifer vorgehen, hat sich enorm professionalisiert. Penetrationstests und Sicherheitsanalysen helfen, dieser Herausforderung zu begegnen und geeignete Schutzmaßnahmen zu ergreifen.

Interne Risiken entstehen kurioserweise auch durch Innovationen: Anbieter wie SAP erweitern kontinuierlich ihre Plattformen, um ihre Kunden an neuen Geschäftsideen und Prozessinnovationen teilhaben zu lassen. Seit 2004 bietet SAP beispielsweise den sogenannten Java-Stack – eine Technologie, die zunehmend bei der webbasierten Anbindung von Browsern, Smartphones und Tablets zum Einsatz kommt. Wird der Java-Stack vor Inbetriebnahme jedoch nicht ausreichend gehärtet, eröffnen sich neue Angriffsmöglichkeiten.

Solche Sicherheitslücken können schwerwiegende Folgen haben, denn der Verlust unternehmenskritischer Informationen durch Industriespionage oder personenbezogener Daten kann schnell Imageschäden und hohe Kosten verursachen. Zudem fordern sowohl die geltenden gesetzlichen Vorgaben als auch die internen Compliance-Anforderungen ein aktives Sicherheitsmanagement.

Was können Sie tun?

Nicht jedes interne System kann und muss ein Hochsicherheitsbereich werden. Am Anfang jeder Analyse müssen deshalb risikoorientiert die tatsächlich schützenswerten Informationen identifiziert werden. Hierbei geht es vor allem um die Frage, welche Daten essenziell für das Geschäft sind. Folglich richtet sich der Fokus einer Sicherheitsanalyse auf Systeme und Anwendungen, die die schützenswerten Daten speichern und verarbeiten. Sie sind das lohnenswerteste Ziel für Hacker und Wirtschaftsspione.

83 % der Unternehmen glauben, dass ein gezielter Angriff (APT) bei ihnen stattgefunden hat.

Anders stellt sich die Situation für die webbasierten Systeme dar. Zwar gilt auch hier, dass die wirklich sensiblen Daten, wie Konstruktionspläne, Kundenkonditionen und Personaldaten, als erstes geschützt werden müssen. Aber auch ein vermeintlicher „Kinderstreich" wie das Verunstalten der Webseite kann einen enormen Reputationsschaden bedeuten. Hier gilt es vorzubeugen.

Um schnell zu den Lücken in Ihren Systemen zu gelangen, stellen Sie sich einmal folgende Fragen:

- Welche Daten sind überhaupt unternehmenskritisch?
- Wissen Sie, in welchen Systemen diese Daten gespeichert sind?
- Haben Sie die Sicherheit Ihres SAP-Systems schon einmal testen lassen?
- Wann haben Sie zuletzt einen Angriffsversuch aus dem Internet simuliert?
- Wie gut sind Ihre Hintertüren gesichert? (Eine hohe Anwendungssicherheit allein ist nicht ausreichend. Wenn Betriebssysteme und Datenbanken nicht ähnlich gut gesichert sind, kommt der Angreifer durch die Hintertür.)

Unser Angebot

Der bestmögliche Schutz geschäftskritischer Daten kann nur durch eine konsequente Absicherung der vollständigen System-Plattformen erreicht werden. Wir unterstützen Sie dabei, die Sicherheit Ihrer Daten zu erhöhen – beispielsweise durch:

- Penetrationstests aus dem Internet, bei denen wir die Sicht des externen Angreifers simulieren
- Interne Sicherheitsanalysen für kritische Systeme, wie Webanwendungen, SAP- und weitere IT-Anwendungen, aus der Sicht eines Innentäters
- Analysen der Sicherheit von IT-Infrastrukturen, wie Betriebssystemen, Datenbanken, Netzwerkkomponenten, mobilen Systemen und Smartphones
- Unterstützung bei der Inventarisierung Ihrer geschäftskritischen Daten
- Prüfung und Design von Sicherheitsarchitekturen
- Weitere spezialisierte Sicherheitsdienstleistungen, wie Quellcode-Reviews, Mobile Security, App-Sicherheit, Metadaten, Zoning-Konzepte etc.

Darüber hinaus unterstützen wir Sie bei der dauerhaften Sicherung Ihrer Systeme und Daten. Wir konzipieren nachhaltige Prozesse und beraten bei der Einführung der notwendigen Verantwortlichkeitsstrukturen in Ihrem Unternehmen.

BCM-Szenarien der Zukunft: Nie wieder ohne Cyberrisiken?

> Es kommt nicht darauf an, die Zukunft vorauszusehen, sondern auf die Zukunft vorbereitet zu sein.
>
> Perikles

Unternehmerisches Handeln ist eng verbunden mit dem Streben nach wirtschaftlichem Gewinn und Rentabilität. Dabei wird häufig die Frage nach unternehmenskritischen Risiken vernachlässigt beziehungsweise ohne weitere Analyse akzeptiert. Der Grundsatz der Unternehmensfortführung gilt nicht nur als Prinzip der Wirtschaftsprüfung, sondern ist auch in den Köpfen von Führungskräften fest verankert.

Risiken mit einer Eintrittswahrscheinlichkeit von unter einem Prozent blenden Unternehmen häufig aus, obwohl das Schadensausmaß enorm sein kann. Cyberrisiken gehören zu den Krisenszenarien der Zukunft: Denn der Angriff muss nicht nur das Unternehmen selbst treffen – Abhängigkeiten ergeben sich auch mit Blick auf externe Dienstleister, wie Telekommunikationsanbieter oder Energieversorger.

50 % der Unternehmen haben keinen Notfallplan für IT-Sicherheitsvorfälle.

Was können Sie tun?

KPMG-Mandanten fragen regelmäßig: Sind wir auf solche Szenarien vorbereitet? Die Antwort ist leider erschreckend. In den Schubladen der Unternehmen finden sich häufig veraltete Notfallpläne, nicht ausreichend kommunizierte Notfallprozesse, eine die Notfallübung ignorierende Belegschaft und ein BCM-Verantwortlicher, der mit seiner halben Stelle zu 95 Prozent in wichtigen anderen Projekten eingebunden ist. Dazu kommen Betriebsunterbrechungen, die man im „Gerade-noch-mal-gut-gegangen-Zustand" feiert, aber nicht auswertet, oder subjektive Bewertungen einzelner Geschäftsbereiche, die mit viel Aufwand zusammengetragen, jedoch Entscheidungsträgern weitgehend unbekannt sind. Einmal mehr kommt es also darauf an, Ihre Sicherheit zu hinterfragen:

- Kennen Sie die Geschäftsprozesse, die auch im Krisenfall unbedingt aufrechterhalten werden müssen?
- Wissen Sie, von welchen Ressourcen die Funktionsfähigkeit Ihrer Prozesse abhängt?
- Kennen Sie die Lücken und Schwächen in Ihren aktuellen Notfallplänen?

Unser Angebot

Wir unterstützen Sie dabei, den Umsetzungsstand des Business Continuity Managements in Ihrem Unternehmen zu ermitteln. Unsere BCM-Reifegradanalyse liefert Ihnen

- einen transparenten Benchmark auf Basis des international anerkannten Standards ISO 22301 und
- Transparenz über bestehende Lücken mit konkreten Handlungsempfehlungen.

Wir stellen Ihre Notfallkonzeption neu auf – und schneidern diese auf relevante Szenarien sowie deren Auswirkungen auf Ihre Geschäftsprozesse und Services zu. Zusammen mit Ihnen

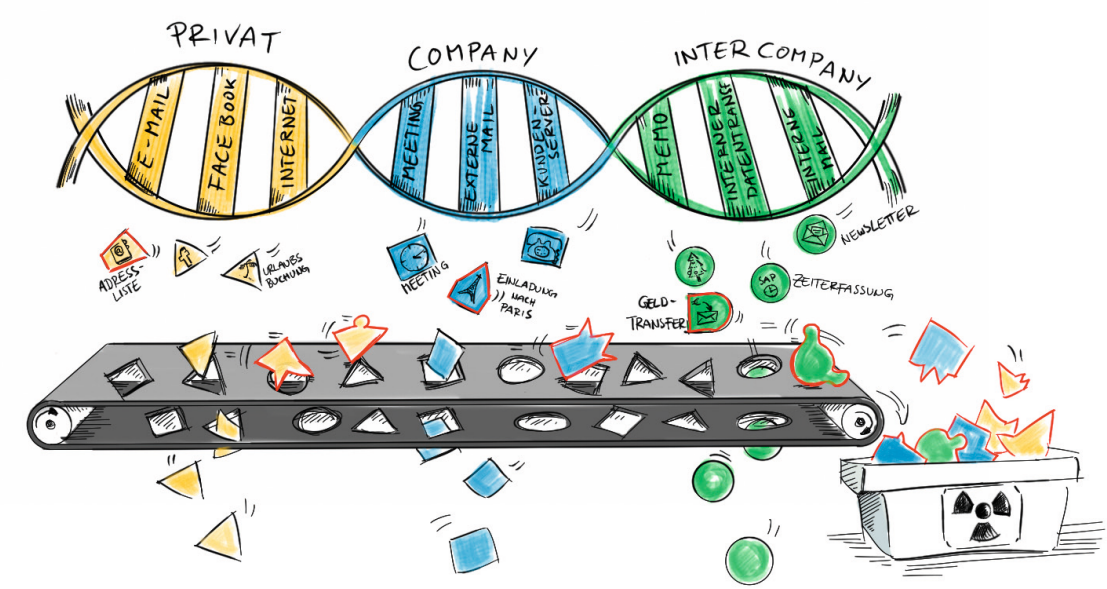
- entwickeln wir eine Methode zur Business Impact-Analyse (BIA)
- identifizieren wir kritische Geschäfts- und Serviceprozesse und priorisieren diese
- definieren wir relevante Wiederanlaufwerte (RTO – Recovery Time Objective)
- schaffen wir Transparenz über die Abhängigkeiten zwischen Geschäftsprozessen und Services.

6 Authorisation Verification: Haben Sie den Datenzugriff im Griff?

> Wenn du im Recht bist, kannst du dir leisten, die Ruhe zu bewahren; und wenn du im Unrecht bist, kannst du dir nicht leisten, sie zu verlieren.
>
> Mahatma Gandi

Sicherheit und Schutz von Informationen zählen nicht erst seit der NSA-Affäre zu den Top-Themen in Unternehmen. Regelmäßige Meldungen über den Diebstahl sensibler Unternehmensdaten zeigen, dass sowohl Kunden- als auch Finanz-, Forschungs- und Entwicklungsdaten sowie andere kritische Informationen immer wieder Ziel von externen wie internen Angriffen sind.

Unsere Untersuchungen haben gezeigt, dass viele Datenverluste und -manipulationen erst durch Schwächen im Berechtigungsmanagement möglich oder zumindest begünstigt werden. Nicht umsonst sind Prüfungen, welche Personen mit welchen Berechtigungen auf welche Daten zugreifen können, ein zentraler Bestandteil des internen Kontrollsystems. Hierin liegt regelmäßig auch ein Schwerpunkt bei unternehmensinternen oder externen Prüfungen.



In den USA wurden 2012 über
12 Millionen Menschen
Opfer von Identitätsdiebstahl.

Was können Sie tun?

Ein KPMG-Mandant stand vor der Herausforderung, Auskunft zur korrekten Berechtigungsvergabe für mehrere kritische Anwendungen zu geben. Durch eine automatisierte Berechtigungsprüfung versetzte KPMG den Kunden innerhalb weniger Tage in die Lage, Berechtigungen der Nutzer zu bereinigen und wesentliche Funktionstrennungsaspekte sicherzustellen. Aufgrund dieser Auswertungen erhielt das Unternehmen

- Transparenz über die Qualität seines Berechtigungsmanagements
- Nachweise über die Wirksamkeit der Zugriffsschutzkontrollen
- eindeutige Hinweise auf operative und prozessuale Schwachstellen und Risiken sowie
- gezielte Handlungsempfehlungen zur Beseitigung identifizierter Schwachstellen und Risiken.

Zusätzlich konnten die Ergebnisse auch für die Einschätzung der Wirksamkeit des internen Kontrollsystems im Rahmen der Jahresabschlussprüfung verwendet werden. Stellen Sie Ihre Zugriffsberechtigungen anhand folgender Fragen auf den Prüfstand:

- Werden vorgeschriebene Abläufe bei Eintritt, Veränderung und Austritt von Mitarbeitern eingehalten?
- Sind Berechtigungskonzepte und Funktionstrennungen angemessen umgesetzt?
- Ist die Vergabe kritischer Systemberechtigungen geregelt?
- Werden rechtliche und interne Compliance-Anforderungen eingehalten?
- Existieren aktive Benutzer im System, die das Unternehmen eigentlich längst verlassen haben?
- Kennen Sie die Benutzerprofile und Berechtigungen Ihrer externen Dienstleister?

Unser Angebot

Wir fokussieren die automatisierte Berechtigungsprüfung gezielt und flexibel auf ausgewählte kritische Systeme und Anwendungen oder auf bestimmte Risiken. Der Ansatz ermöglicht uns

- automatisierte Auswertungen und Analysen in hoher Qualität
- schnelle und kostengünstige Überprüfungen von Best Practice-Kontrollen und kritischen Individualkontrollen
- Lieferung konkreter, direkt in Maßnahmen umsetzbarer Ergebnisse mit überschaubarem Aufwand.

Wir unterstützen Sie zudem dabei, die Strukturen und Prozesse zu etablieren, die für eine gleichbleibend hohe Qualität des Berechtigungsmanagements unabdingbar sind.

Security Monitoring: Und die Cyberattacken prallen an Ihrem Unternehmen ab?

Die IT-Sicherheitslandschaft hat sich verändert. Die Folge: Technologien zum Schutz der Informationen im Unternehmen müssen sich ebenfalls ändern. Organisationen können sich nicht mehr nur auf präventive Sicherheitsmaßnahmen, wie Firewalls, Anti-Viren-Programme und Benutzer-Authentifizierungssysteme, verlassen, um sich ausreichend vor aktuellen und hochentwickelten Angriffen zu schützen.

> Am wichtigsten ist die Begabung, aus schlechten Erfahrungen wirklich etwas zu lernen.
>
> James Thurber

Tatsache ist, dass kapitalkräftige und fachkundige Angreifer herkömmliche präventive Sicherheitssysteme leicht umgehen können. Unternehmen müssen daher ihre Fähigkeiten zur Früherkennung, Nachverfolgung und Reaktion verbessern, um dieser Entwicklung Rechnung zu tragen. Ein effektives Security Monitoring ist die Basis dafür – und von zentraler Bedeutung für die Verteidigung gegen hochentwickelte Bedrohungen.

Bei der Analyse von 900 erfolgreichen Angriffen fand man in **90 %** der Fälle Hinweise in den Log-Dateien, wobei nur **5 %** der Unternehmen den Angriff erkannt haben.

Was können Sie tun?

Das Know-how aus Forschung und Entwicklung stellt für unsere Mandanten in der chemischen und pharmazeutischen Industrie den Wert des Unternehmens dar. Investitionen in diesen Bereichen sind zu schützen, um langfristig erfolgreich zu agieren. Vor diesem Hintergrund evaluieren wir für Mandanten die Möglichkeiten netzwerkbasierter Analysen von Anomalien, um Industriespionage gezielt aufzudecken beziehungsweise zu verhindern. Der Fokus liegt dabei auch auf der rechtlichen Zulässigkeit solcher Überwachung im Rahmen nationaler und europäischer Datenschutzbestimmungen. Welche Antworten haben Sie in diesem Zusammenhang auf folgende Fragen:

- Können Sie im Unternehmen verschlüsselte ZIP-Dateien als E-Mail-Anhang an Dritte versenden?
- Setzt Ihr Unternehmen netzwerkbasierte Analysetechniken ein?
- Gibt es Betriebsvereinbarungen zur Auswertung und Nachverfolgung des Nutzungsverhaltens Ihrer IT?
- Werden Ihre IT-Systeme rund um die Uhr überwacht?

Unser Angebot

Wir unterstützen Sie dabei, Verfahren zur netzwerkbasierten Sicherheitsanalyse zu konzipieren und gesetzeskonform einzusetzen. Wir beraten und unterstützen Sie bei der

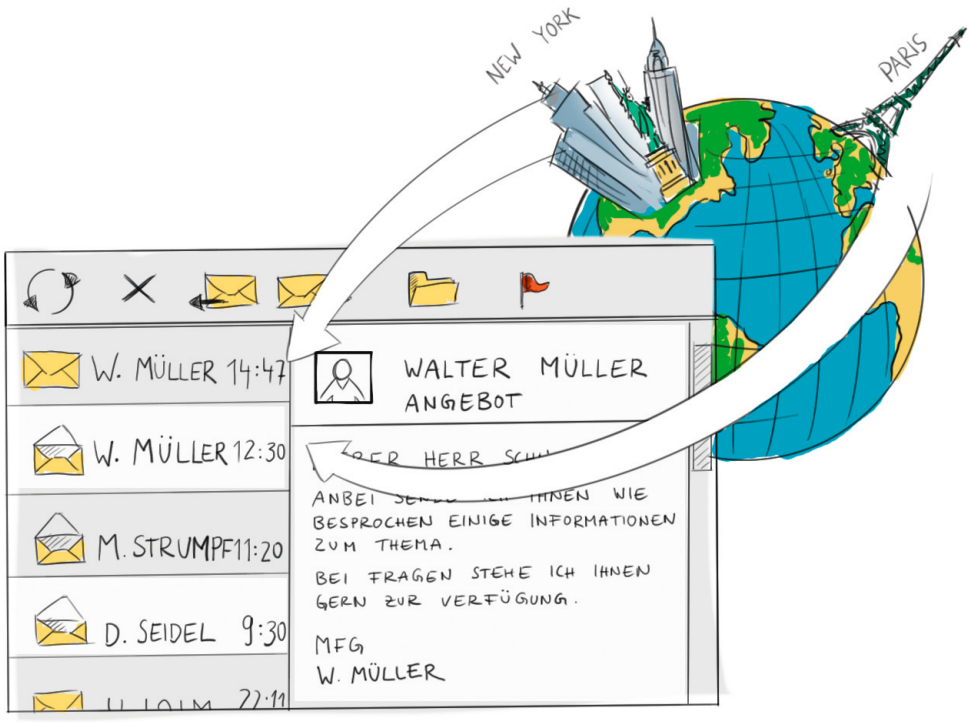
- Anbieterauswahl von Security Monitoring-Technologien
- Abstimmung relevanter Anomalien, Customizing der Regeln und
- Beratung zur Erfüllung rechtlicher Rahmenbedingungen, bezogen auf Datenschutz und Mitbestimmungspflichten.

Zertifizierungen: Kann ein Siegel Sicherheit geben?

> Wer sein Ziel kennt, kann entscheiden. Wer entscheiden kann, findet Ruhe. Wer Ruhe findet, ist sicher. Wer sicher ist, kann verändern.
>
> Konfuzius

Sicherheit im Unternehmen ist kein Zustand. Sie ist immer als Prozess zu verstehen, der einer kontinuierlichen Entwicklung unterliegt. Dabei sind die strenge Orientierung an einem anerkannten Standard für ein Informationssicherheits-Managementsystem (ISMS) sowie die Kontrolle der Einhaltung definierter organisatorischer Rahmenbedingungen wesentliche Erfolgsfaktoren.

Kunden, Regulierungsbehörden und die Organe der Gesellschaft verlangen nach einem transparenten Status quo zur Informationssicherheit. Die Orientierung an einem etablierten und international anerkannten Standard wie ISO/IEC 27001 kann dabei zum Wettbewerbsfaktor werden. Denn immer häufiger wird eine Zertifizierung oder zumindest die enge Orientierung an ISO/IEC 27001 gefordert. Aber nicht nur nach außen sorgt die Umsetzung der Vorgaben für Vorteile.



Deutschen Unternehmen
entstand 2012 ein Schaden von
43 Milliarden Euro
durch Cyberkriminalität.

Auch aus Sicht der Organe der Gesellschaft ergibt sich durch die externe Überprüfung der Informationssicherheits-Organisation und -maßnahmen ein Enthaftungsnachweis im Hinblick auf ihre Organisations- und Überwachungsverpflichtung.

Was können Sie tun?

Ein langjähriger KPMG-Mandant – ein IT-Dienstleister – lässt bereits seit Jahren seine IT-Prozesse für rechnungslegungsrelevante Systeme von uns prüfen. Die Ausschreibungen seiner Kunden enthalten verstärkt die Forderung zur Umsetzung von ISO/IEC 27001. Basierend auf den existierenden Maßnahmen haben wir den Mandanten beim Aufbau des Managementsystems unterstützt, sodass er sich innerhalb von nur zwölf Monaten zertifizieren lassen konnte. Bewerten Sie einmal die Situation in Ihrem Unternehmen:

- Fordern Aufsichtsbehörden oder Kunden von Ihnen eine Orientierung nach ISO/IEC 27001?
- Wollen Sie wissen, wie weit Sie von einer möglichen Zertifizierung entfernt sind?
- Haben Sie bereits Managementsysteme (wie ISO 9000, ISO 20000) implementiert und möchten Sie um das Thema Informationssicherheit erweitern?

Unser Angebot

Wir unterstützen Sie dabei, Ihre Informationssicherheit konform mit dem Standard ISO/IEC 27001 aufzubauen. Dazu bieten wir Ihnen

- Reifegradanalyse Ihrer Informationssicherheits-Organisation
- Ableitung konkreter Handlungsempfehlungen für Ihre Zertifizierungs-Roadmap
- Schulung und Weiterbildung (ISO/IEC 27001 Lead Auditor und Lead Implementer).

Mit der KPMG Cert GmbH sind wir in der Lage, Ihr Informationssicherheits-Managementsystem nach ISO/IEC 27001 zu zertifizieren.

Kontakt

KPMG AG
Wirtschaftsprüfungsgesellschaft

Uwe Bernd-Striebeck
Partner, Security Consulting
T +49 201 455-6870
uberndstriebeck@kpmg.com

Wilhelm Dolle
Partner, Security Consulting
T +49 30 2068-2323
wdolle@kpmg.com

www.kpmg.de