Informationssicherheit

Selbsteinschätzung Ihrer Ist-Situation

Informationen stellen in den meisten Unternehmen einen signifikanten Unternehmenswert dar. Aus diesem Grunde ist es wichtig, dass angemessene Maßnahmen zum Schutz der Informationen geplant, aufgebaut und regelmäßig überprüft werden. Dieser Fragebogen soll ihnen eine erste Einschätzung dafür geben, ob die durchgeführten Security Maßnahmen in ihrer Organisation dem Schutzbedarf genügen.

Beantworten Sie die folgenden Fragen nach Ihrem aktuellen Kenntnisstand, auch wenn er nicht unbedingt den tatsächlichen Gegebenheiten entspricht. Auch Unsicherheiten bzgl. der vorhandenen Informationssicherheit sind ein Zeichen dafür, diesem Thema erneut Aufmerksamkeit zu schenken. Die Texte unter den Fragen sollen Ihnen die Beantwortung erleichtern und die Fragestellung erläutern.

.

1. Wie handhaben Sie in ihrer Organisation die Richtlinien zur Informationssicherheit?	
1. Es gibt ein gut dokumentiertes, detailliertes und allgemein bekannt gemachtes Richtlinienwerk.	☐
2. Die Richtlinien sind gut dokumentiert, aber nicht allgemein bekannt.	☐
3. Die Richtlinien sind eher abstrakt oder unvollständig dokumentiert.	☐
4. Ist mir nicht bekannt bzw. wir haben keine Richtlinien zur Informationssicherheit.	☐

Das Richtlinienwerk zur Informationssicherheit oder die Security Policy stellt das zentrale Dokument dar, das beschreibt, wie das Management beabsichtigt, die Informationssicherheit zu betreiben und welche Unterstützung seitens der Organisationsleitung dazu bereitgestellt wird. Es stellt den Ankerpunkt für alle weiterführenden Sicherheitsmaßnahmen dar und soll dafür Sorge tragen, dass die einzelnen Maßnahmen sich sinnvoll zu einem ganzheitlichen Sicherheitskonzept zusammenfügen. Die Security Policy muss in der gesamten Organisation verbreitet werden, damit alle Mitarbeitenden die Leitlinien der Informationssicherheit kennen.

Um nachhaltig die Informationssicherheit im Unternehmen sicherstellen zu können, ist es notwendig, ein dediziertes Information Security Management zu etablieren und auch mit entsprechenden personellen und finanziellen Mitteln auszustatten. Der oder die Sicherheitsbeauftragte/n müssen frühzeitig in die Planung neuer Vorhaben einbezogen werden, um rechtzeitig nachteilige Auswirkungen auf die Informationssicherheit auszuschließen oder rechtzeitig geeignete Schutzmaßnahmen planen und einleiten zu können.

2. Wie wird sichergestellt, dass die Informationssicherheit immer dem aktuellen Schutzbedarf angepasst wird?	
1. Es gibt ein Information Security Management, das mit ausreichend Zeit- und Geldbudget ausgestattet ist.	☐
2. Es gibt einen Sicherheitsbeauftragten, der diese Aufgabe neben seiner normalen Tätigkeit übernimmt.	☐
3. Die Aktualisierung der Sicherheitsmaßnahmen wird bei Bedarf von der IT übernommen.	☐
4. Es gibt kein definiertes Vorgehen.	☐

3. Wissen Sie, wie kritisch die einzelnen Datengruppen/Informationen innerhalb ihrer Organisation hinsichtlich Vertraulichkeit, Verfügbarkeit und Integrität sind?

1. Wir haben eine vollständige Klassifikation aller Datenbestände in dieser Hinsicht.	☐
2. Die wesentlichen Datenbestände sind dokumentiert und klassifiziert.	☐
3. Es gibt keine durchgängige Dokumentation und Klassifikation der Datenbestände.	☐
4. Wir brauchen keine Klassifizierung der Datenbestände.	☐

Nicht alle Datenbestände innerhalb einer Organisation sind hinsichtlich der genannten Aspekte gleich kritisch. Während für Grunddaten in der Regel eine hohe Klassifizierung vorzunehmen ist, können Sekundärdaten häufig als weniger kritisch betrachtet werden, da sie sich meistens aus den Grunddaten rekonstruieren lassen. Die Klassifizierung ist deshalb wichtig, weil sichergestellt werden muss, dass keine kritischen Daten unbeachtet bleiben, und zugleich um hohe Sicherungskosten für weniger kritische Daten zu vermeiden.

4. Inwieweit sind Ihre Mitarbeiter/innen hinsichtlich ihrer Verantwortung für Informationssicherheit unterrichtet?

1. Zu jeder Rolle im Unternehmen gehören auch entsprechende Sicherheitsvorschriften und es gibt regelmäßige Informationen und Schulungen.	☐
2. Mitarbeiter werden auf die allgemeinen Vorschriften zur Informationssicherheit verpflichtet.	☐
3. Die Vorschriften zur Informationssicherheit sind zugänglich und es wird darauf hingewiesen.	☐
4. Es gibt keine spezielle Unterrichtung der Mitarbeiter.	☐

Zu jeder Arbeitsplatz- oder Rollenspezifikation sind auch die am jeweiligen Arbeitsplatz geltenden Sicherheitsrichtlinien zu hinterlegen. Zudem muss in der Rollenbeschreibung auf etwaige Besonderheiten oder besondere Verantwortungen hinsichtlich der Informationssicherheit hingewiesen werden. Sind über die allgemeinen Richtlinien hinaus keine Besonderheiten zu beachten, dann sollte das ebenfalls ausdrücklich vermerkt werden. Im Übrigen ist laut Arbeitsrecht eine solche Arbeitsplatz- oder Rollenbeschreibung vorgesehen, um Unklarheiten, die später ggf. vor dem Arbeitsgericht ausgefochten werden müssen, im Vorfeld auszuräumen. Daneben sollte auch eine regelmäßige Sensibilisierung Ihrer Mitarbeiter für Informationssicherheit stattfinden.

5. Sind Datenverarbeitungssysteme und Datenbestände gegen Diebstahl oder physische Zerstörung gesichert?

1. Sind alle Datenverarbeitungsanlagen, auf denen sich kritische Daten sowie Datenträger mit solchen Daten befinden, in speziell abgesicherten Räumen mit entsprechenden Alarmvorrichtungen?	☐
2. Server und Netzwerkkomponenten sind in verschlossenen Räumen oder Schränken, Datenbestände sind aber möglicherweise auch auf PCs oder auf unregistrierten Datenträgern.	☐

3. Es gibt eine Weisung zur Aufbewahrung von Datenträgern, aber die Systeme sind nicht gesondert geschützt. ☐

4. Es gibt keine speziellen physischen Schutzmaßnahmen. ☐

In vielen Unternehmen ist es einfacher einen ganzen Server mitzunehmen als zu versuchen in diesen über Netze einzudringen und die Daten zu entwenden. Daneben nimmt bei Einbruchsdiebstählen der Vandalismus stetig zu, so dass man bei ungeschützter Unterbringung eine Zerstörung riskiert. Abgesehen davon kann es natürlich auch durch äußere Einflüsse zu solchen Zerstörungen kommen, wie etwa durch Brand, Wassereinbruch, Leitungswasserschäden, Störungen auf dem Stromnetz, Blitzeinschlag, ...

6. Existieren zu allen verwendeten Verfahren der Datenverarbeitung und Datenübermittlung

Betriebshandbücher, Vorgehensvorschriften und Sicherheitsrichtlinien?

1. Ja, es ist ein vollständig dokumentiertes Systems- und Communications-Management etabliert. ☐

2. Es gibt Betriebshandbücher, aber sie werden nicht regelmäßig überprüft. ☐

3. Es gibt nicht zu jedem System eine Betriebsdokumentation. ☐

4. Es gibt keine aktuellen Betriebshandbücher oder sonstige Dokumentation. ☐

Systemadministration und Betrieb sind sehr sensible Bereiche im Hinblick auf die Informationssicherheit. Zum einen ist es wichtig auf kontrollierte Weise die System- und Netzwerksicherheit auf einem aktuellen Stand zu halten und zum anderen besteht auf Systemebene prinzipiell die Möglichkeit auf alle Daten zugreifen zu können. Aus diesem Grund ist es wichtig, die Abläufe in diesem Bereich gut zu regeln und regelmäßig zu überprüfen.

Ein so genanntes rollenbasiertes Zugriffskontrollsystem stellt die anerkannt beste Variante dar Zugriffsrechte zuverlässig zu verwalten. Durch die zentrale Verwaltung der Rollen verbunden mit der Möglichkeit der zentralen und dezentralen Rollenzuordnung, ist eine vollkommen transparente Rechtevergabe möglich. Zudem werden die normalen Vorgänge des Personalmanagements effektiv unterstützt, da Eintritte, Funktionsänderungen und Austritte immer mit einer Rollenzuordnung oder -sperrung realisiert werden können.

7. Wie wird bei Ihnen die Zugriffskontrolle zu Applikationen und Daten geregelt?

1. Wir haben ein vollständig rollenbasiertes Zugriffsmanagement. ☐

2. Zugriffsrechte werden anhand der Tätigkeit bzw. Zugehörigkeit zu einer Arbeitsgruppe vergeben. ☐

3. Es gibt einige Grundberechtigungen die jede/r erhält, der Rest wird ad hoc per Antrag geregelt. ☐

4. Alle Berechtigungen werden ad hoc ohne große Formalitäten vergeben. ☐

8. In jedem Betrieb sind Wartungs-, Weiterentwicklungs-und Anpassungsarbeiten an den IT-Lösungen erforderlich.

Gibt es dafür ein klares Vorgehenskonzept?

1. Alle Wartungs- und Entwicklungsarbeiten werden unter strenger Qualitätskontrolle vorgenommen. ☐

2. Alle Wartungs- und Entwicklungsarbeiten werden vom Projektmanagement begleitet.	☐
3. Größere Anpassungen erfolgen unter Projektmanagementkontrolle, kleinere werden ad hoc durchgeführt.	☐
4. Anpassungen werden ohne geregeltes Vorgehen vorgenommen.	☐

Jede Anpassung auch kleine Korrekturen an Parametrisierungen und Konfigurationen stellen einen Eingriff in laufende Systeme dar und können potenzielle Schwachstellen bilden oder das System destabilisieren. Folglich sollten alle Eingriffe geplant, kontrolliert und dokumentiert werden. Wo eigene Software-Entwicklung stattfindet, sollte ein Qualitätssicherungskonzept eingeführt werden.

9. Wie wird in Ihrer Organisation mit drohenden und eingetretenen Sicherheitsvorfällen umgegangen?

1. Wir informieren uns regelmäßig mindestens einmal pro Woche über mögliche neue Bedrohungen und bekannt gewordene Schwachstellen in den von uns eingesetzten Systemen, führen Sicherheitsaktualisierungen automatisch oder zumindest zeitnah aus und gehen den Ursachen von eingetretenen Vorfällen nach, um sie möglichst beseitigen zu können.	☐
2.Bei eingetretenen Sicherheitsvorfällen suchen wir die Ursachen und beheben sie möglichst.	☐
3. Schäden von Sicherheitsvorfällen werden behoben.	☐
4. Wir haben kein explizites Konzept für solche Vorfälle	☐

Sicherheitsvorfälle können nicht vollständig ausgeschlossen werden. Mit einem proaktiven Incident Management, also der regelmäßigen aktuellen Information über Sicherheitsrisiken und der darauf folgenden zeitnahen Umsetzung von entsprechenden Gegenmaßnahmen wie dem Einspielen von Aktualisierungen können Gefahren in diesem Bereich jedoch deutlich gesenkt werden.

Ein Notfallvorsorgekonzept kann im Zweifelsfall über das Überleben eines Unternehmens entscheiden. Analysen von Schadensfällen zeigen, dass die Wahrscheinlichkeit einen Schadensfall zu überstehen, mindestens doppelt so hoch ist bei Unternehmen, die einen detaillierten und regelmäßig aktualisierten Notfallplan haben. Im Fall der Abwendung von kurz- und mittelfristigen Schäden sind die Vorteile noch deutlicher, da durch einen guten Notfallplan eine schnelle und zielgerichtete Schadenseindämmung und -beseitigung klar begünstigt wird.

10. Haben Sie ein aktuelles Notfallvorsorgekonzept, das regelmäßig überprüft wird?

1. Es existiert ein detailliertes und modulares Notfallvorsorgekonzept, das mindestens einmal pro Jahr überprüft wird.	☐
2. Es existiert ein Notfallvorsorgekonzept, aber es wird nicht regelmäßig überprüft.	☐
3. Es existieren allgemeine Notfallregelungen, die aber nicht sehr detailliert sind.	☐
4. Es gibt bisher kein Notfallkonzept.	☐

11. Sind Ihre Informationsverarbeitungsverfahren konform mit geltenden gesetzlichen Regelungen, technologischen und regulativen Rahmenbedingungen?

1. Alle Verfahren werden regelmäßig auf Konformität hin überprüft und bei Bedarf angepasst. Bei Änderungen von Rahmenbedingungen werden deren Relevanz geprüft und ggf. entsprechende Anpassungen veranlasst. ☐

2. Vor Inbetriebnahme von Lösungen werden sie auf Verträglichkeit geprüft. ☐

3. Wenn Änderungen in den Rahmenbedingungen bekannt werden, wird ihre Relevanz geprüft, es wird aber nicht aktiv nach solchen Änderungen Ausschau gehalten. ☐

4. Hinsichtlich der Konformität ist nichts bekannt. ☐

Alle Verarbeitungen von Informationen müssen mit den Rahmenbedingungen verträglich sein. Bei gesetzlichen Rahmenbedingungen ist das relativ schnell einsichtig. So müssen z.B. für die Verarbeitung von personenbezogenen Daten die Regelungen des Bundesdatenschutzgesetzes (BDSG) berücksichtigt werden. Nicht so offensichtlich ist die Bedeutung der technologischen Konformität. Ein wesentlicher Aspekt ist hierbei die Wartung von eingesetzter Standardsoftware. Jedes dieser Produkte erreicht irgendwann das Ende seiner Wartungsperiode. Danach werden nur noch neuere Versionen gewartet.

Für Fehler, die nach dem Auslaufen der Wartung auftreten und die ggf. auch noch ein Sicherheitsproblem aufwerfen, erfolgt keine Korrektur mehr und auch jegliche Haftung ist dafür ausgeschlossen.

Auswertung

Zählen Sie wie oft Sie jeweils die Antwort 1, 2, 3 oder 4 gewählt haben und tragen Sie dies in die nachfolgende Tabelle ein.

Antwort 1	Antwort 2	Antwort 3	Antwort 4

Bewertung

- Sollten Sie in Spalte 4 einen Wert größer 0 haben, dann besteht dringender Handlungsbedarf. Mit einer Analyse und anschließender Auswertung können wir Ihnen detailliert sagen, welche Maßnahmen dringend erforderlich sind und welche weiteren sinnvoll wären.
- Bei einem Wert größer 0 in Spalte 3 ist zwar in allen Bereichen ein minimales Sicherheitsmanagement vorhanden, aber es besteht einiges Verbesserungspotential. Eine Beeinträchtigungsanalyse, die wir in einem Interview erheben können, kann Ihnen aufzeigen, in welchen Bereichen bei Ihnen die höchsten Risiken bestehen. Mit der anschließenden Auswertung erfahren Sie, welche Maßnahmen sinnvoll sind, um die Risikosituation auf ein sinnvolles Maß einzustellen.
- Alle Werte in Spalten 1 und 2 bedeutet, dass Sie schon ein gutes Sicherheitsmanagement betreiben. Hier empfehlen wir eine regelmäßige -sinnvollerweise jährliche- Überprüfung der Situation, um das Sicherheitsniveau hoch zu halten.