Analyse | Cyber-Quick-Check KMU

Organisation

Organisation der Informationssicherheit

Zur Durchsetzung von Sicherheitsmaßnahmen in einem Unternehmen ist es wichtig, dass die Unternehmensleitung die Verantwortung hierfür übernimmt. Zusätzlich sollten für die Abgrenzung der Aufgabengebiete, aber auch zur Vermeidung von Zuständigkeitslücken die Verantwortlichkeiten für alle wesentlichen Aufgaben, insbesondere im Informationssicherheitsprozess, nachvollziehbar geregelt sein.

Unser Topmanagement hat sich schriftlich verpflichtet, die Gesamtverantwortung für die Informationssicherheit wahrzunehmen. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?
Wir haben klare Verantwortlichkeiten für unsere Informationssicherheit definiert. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?
Wir haben das Prinzip der Funktionstrennung umgesetzt, d.h. Ausführung und Kontrolle der Aufgaben zur Gewährleistung der Informationssicherheit sind voneinander getrennt. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?

Richtlinien

Ausschließlich mündlich gegebene Anweisungen sind in der Regel nicht nachhaltig und geraten schnell in Vergessenheit. Daher sollten Richtlinien und Anweisung in schriftlicher Form dokumentiert werden. Besonders bei wachsenden Unternehmen muss frühzeitig mit einer solchen Dokumentation begonnen werden, um langfristig die Arbeitsaufwände zur Pflege der Dokumentation zu minimieren und die Verfügbarkeit und Aktualität der Richtlinien und Anweisungen sicherstellen zu können.

Wir haben eine Richtlinie für unsere Mitarbeiter, in der definiert ist, wie mit der IT und den Daten des Unternehmens umgegangen werden muss. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?
Die private Nutzung unserer Unternehmens-IT ist in einer Richtlinie geregelt. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?
Wir haben eine Richtlinie für unsere IT-Dienstleister, in der definiert ist, wie mit der IT und den Daten des Unternehmens umgegangen werden muss. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?

Analyse | Cyber-Quick-Check KMU

Personal

Informiertes und geschultes Personal ist die Grundlage einer sicheren Durchführung von Geschäftsprozessen in Unternehmen. Neben der Information des Personals über die etablierten Prozesse, unternehmensspezifische Regelungen und Handlungsanweisungen sind insbesondere regelmäßige Schulungen zu IT-Sicherheitsmaßnahmen erforderlich, um eine Verbesserung des IT-Sicherheitsniveaus zu erreichen.

Alle internen und externen Mitarbeiter kennen die betreffenden Regelungen zur Informationssicherheit. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?
Alle internen und externen Mitarbeiter haben eine schriftliche Vertraulichkeitserklärung abgegeben. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?
Alle internen und externen Mitarbeiter werden regelmäßig über unsere Maßnahmen zur Informationssicherheit informiert. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?

* Feld muss ausgefüllt werden

Zugänge

Die einmalige Umsetzung von IT-Sicherheit bildet nur einen kurzfristigen Schutz des Unternehmens. So schnell, wie sich IT-Systeme ändern, so schnell ändern sich auch die Bedrohungen für ein Unternehmen. Nur durch regelmäßige Aktualisierung der Informationen und durch die regelmäßige Anpassung der Schutzmaßnahmen können diese einen längerfristigen Schutz des Unternehmens bieten. Hierfür müssen entsprechende Prozesse zur Aktualisierung der Informationen, aber auch zur Anpassung der Maßnahmen bestehen.

Zugänge für unsere IT-Infrastruktur werden konsequent nur gewährt, wenn sie für die Aufgabenerfüllung notwendig sind. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?
Administrative Zugänge sind ausschließlich unseren Administratoren vorbehalten. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?
Administrative Zugänge werden von uns regelmäßig nach einem festgelegten Turnus auf deren Notwendigkeit überprüft. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?

* Feld muss ausgefüllt werden

Analyse | Cyber-Quick-Check KMU

Technik

Mobile Geräte

Die Anzahl der genutzten Anwendungen auf mobilen Geräten nimmt in den Unternehmen stetig zu. Deshalb ist es insbesondere hier wichtig, sehr genau darauf zu achten, wie man die Unternehmensdaten schützen kann. Mobile Geräte können besonders leicht in die falschen Hände geraten.

Wir haben eine Richtlinie, in der der Umgang mit mobilen Geräten festgelegt ist. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?
Die Daten auf unseren mobilen Geräten sind vor unberechtigtem Zugriff geschützt. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Kein Angabe	?
Im Fall eines Verlust oder Diebstahles eines mobilen Gerätes wissen unsere Nutzer was zu tun ist. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?

* Feld muss ausgefüllt werden

Mobile Datenträger

Mobile Datenträger sind aufgrund ihrer exponierten Nutzungsart besonders gefährdet. Deshalb ist es notwendig, die damit verbundenen Risiken angemessen zu behandeln.

Wir haben festgelegt, welche Informationen des Unternehmens auf mobilen Datenträgern, wie z.B. USB-Sticks, CD-ROMs, DVD-ROMs, Speicherkarten oder mobilen Festplatten gespeichert werden dürfen. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?
Unsere Nutzer werden über die spezifischen Risiken mobiler Datenträger (z. B. Gefahren durch Verlust oder Diebstahl oder durch das Einschleppen von Schadsoftware) informiert und sensibilisert. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?
Unseren Nutzern wird untersagt, mobile Datenträger an unberechtigte Dritte weiterzugeben oder zu verleihen. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?

* Feld muss ausgefüllt werden

Analyse | Cyber-Quick-Check KMU

Netzwerke

IT-Systeme sind in vielen der teilnehmenden Unternehmen eine technische Grundlage für die Realisierung der Geschäftsprozesse. Die IT-Systeme sind über Netze zum Zweck des Datenaustausches sowie der Nutzung bzw. Bereitstellung von Diensten und Anwendungen miteinander verbunden. Zur Anbindung von Unternehmensteilen an anderen Standorten, der Mitarbeiter im Außendienst sowie der Heim- und Telearbeitsplätze und selbstverständlich zur Kommunikation mit den Kunden und Geschäftspartnern werden Netzverbindungen genutzt. Um schutzbedürftige Daten über nicht vertrauenswürdige Netze, wie beispielsweise das Internet, zu übertragen, sind Sicherheitsmaßnahmen zu realisieren. Zur effektiven und effizienten Verwaltung der Netzwerke sind weitere IT-Sicherheitsmaßnahmen erforderlich.

Wir haben den Zugriff auf das Internet durch Schutzmaßnahmen abgesichert. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?
Der Zugriff auf unsere interne IT-Infrastruktur über öffentliche oder drahtlose Netze erfolgt ausschließlich verschlüsselt. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?
Wir führen für besonders kritische IT-Netzwerke regelmäßig Risikoanalysen nach einem festgelegten Turnus durch. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?

IT-Systeme

Informationen sind ein wesentlicher Wert für Unternehmen und müssen daher angemessen geschützt werden. Die meisten Informationen werden heutzutage mit Informationstechnik (IT) erstellt, gespeichert, transportiert oder weiterverarbeitet. Moderne Geschäftsprozesse sind heute in Wirtschaft und Verwaltung ohne IT-Unterstützung längst nicht mehr vorstellbar. Eine zuverlässig funktionierende Informationsverarbeitung ist ebenso wie die zugehörige Technik für die Aufrechterhaltung des Betriebes unerlässlich. Unzureichend geschützte Informationen stellen einen häufig unterschätzten Risikofaktor dar, der für manche Unternehmen existenzbedrohend sein kann. Dabei ist ein vernünftiger Informationsschutz ebenso wie eine Grundsicherung der IT schon mit verhältnismäßig geringen Mitteln zu erreichen.

Wir haben eine Aufstellung aller IT-Systeme unseres Unternehmens, die wir laufend aktualisieren. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?
Wir haben ein Schutzkonzept, wie unsere IT-Systeme abgesichert werden. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?
Wir führen für besonders kritische IT-Systeme regelmäßig Risikoanalysen nach einem festgelegten Turnus durch. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?

* Feld muss ausgefüllt werden

Analyse | Cyber-Quick-Check KMU

Prävention

Sicherheitsvorfälle

Um die Informationssicherheit im laufenden Betrieb aufrecht zu erhalten, ist es notwendig, die Behandlung von Sicherheitsvorfällen im Vorfeld zu konzipieren und einzuüben. Als Sicherheitsvorfall wird dabei ein unerwünschtes Ereignis bezeichnet, das Auswirkungen auf die Informationssicherheit hat und in der Folge große Schäden nach sich ziehen kann. Typische Folgen von Sicherheitsvorfällen können das Ausspähen, die Manipulation oder die Zerstörung von Daten sein. Um Schäden zu vermeiden bzw. zu begrenzen, müssen Sicherheitsvorfälle schnell und effizient bearbeitet werden. Durch ein vorgegebenes und erprobtes Verfahren können Reaktionszeiten minimiert werden.

Wir haben den Begriff „IT-Sicherheitsvorfall" für unser Unternehmen verbindlich definiert. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe ?
Wir haben eine Richtlinie, in welcher der Umgang mit Sicherheitsvorfällen festgelegt ist. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe ?
Im Fall eines Sicherheitsvorfalls wissen unsere Nutzer was zu tun ist. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe ?

* Feld muss ausgefüllt werden

Umgebung

Ein Gebäude umgibt die stationären Arbeitsplätze, die verarbeiteten Informationen sowie die aufgestellte Informationstechnik und gewährleistet für diese somit einen äußeren Schutz. Der Zutritt zu schutzbedürftigen Gebäudeteilen und Räumen ist zu regeln und zu kontrollieren.

Wir haben unsere wichtigen IT-Systeme, wie z.B. Server und Netzwerkverteiler, vor physischem Zugriff gesichert. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe ?
Wir haben unsere wichtigen IT-Systeme, wie z.B. Server und Netzwerkverteiler, vor Brandschäden gesichert. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe ?
Wir haben unsere wichtigen IT-Systeme, wie z.B. Server und Netzwerkverteiler, mit einer unterbrechungsfreien Stromversorgung vor Stromausfällen und Überspannung gesichert. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe ?

* Feld muss ausgefüllt werden

Analyse | Cyber-Quick-Check KMU

Datensicherung

Durch technisches Versagen, versehentliches Löschen oder durch Manipulation können gespeicherte Daten unbrauchbar werden bzw. verloren gehen. Eine Datensicherung soll gewährleisten, dass durch einen redundanten Datenbestand der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen. Um dies zu vermeiden, müssen sich die Unternehmen dem Risiko des Verlusts von Daten bewusst sein und entsprechende Schutzmaßnahmen ergreifen.

Wir schützen uns vor dem Verlust der wichtigsten Unternehmensdaten durch eine Datensicherung. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?
Wir stellen durch regelmäßige Tests nach einem festgelegten Turnus sicher, dass unsere Datensicherung funktioniert. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?
Unsere Datensicherungsmedien werden örtlich getrennt von den gesicherten Systemen aufbewahrt, so dass bei einem Brand oder Wasserschaden nicht beide Datenquellen betroffen sind. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?

* Feld muss ausgefüllt werden

Ausfälle

Ein Ausfall ist ein Schadensereignis, bei dem wesentliche Systeme oder Ressourcen eines Unternehmens nicht wie vorgesehen funktionieren. Hier tritt, abweichend vom Sicherheitsvorfall und Störfall, das Schadensereignis tatsächlich ein. Um Notfällen vorzubeugen, ist der Aufbau und Betrieb eines Notfallmanagement-Verfahrens notwendig. Nur ein geplantes und organisiertes Vorgehen garantiert eine optimale Notfallvorsorge und Notfallbewältigung. Dies verringert die Wahrscheinlichkeit des Auftretens eines Ausfalls sowie dessen Auswirkungen und sichert somit das Überleben des Unternehmens. Es sind geeignete Präventivmaßnahmen zu treffen, die zum einen die Robustheit und Ausfallsicherheit der Geschäftsprozesse erhöhen und zum anderen ein schnelles und zielgerichtetes Reagieren in einem Notfall oder einer Krise ermöglichen.

Wir besitzen für unsere kritischen Systeme Wiederanlaufpläne. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?
Wir besitzen einen Übersichtsplan, aus dem hervorgeht, in welcher Reihenfolge kritische Systeme wieder in Betrieb genommen werden müssen. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?
Unsere Wiederanlaufpläne und unser Übersichtsplan werden so aufbewahrt, dass sie auch bei einem Notfall schnell verfügbar sind. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe	?

* Feld muss ausgefüllt werden

Analyse | Cyber-Quick-Check KMU

IT-Outsourcing und Cloudcomputing

Ein funktionierendes IT-Outsourcing ist eine wesentliche Basis für den Erhalt eines Unternehmens. So werden über Anwendungen die individuellen Geschäftsprozesse eines Unternehmens abgebildet. Besonders kritische IT und Anwendungen sind zu schützen. Entfällt aufgrund schlechter Lizenzen oder Verträge ein kritisches System oder Anwendung so kann die Existenz eines Unternehmens gefährdet sein.

Für jedes IT-Outsourcing Vorhaben haben wir notwendigen Anforderungen an die Sicherheit definiert. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe ?
Für jede Nutzung von Cloud Computing haben wir notwendigen Anforderungen an die Sicherheit definiert. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe ?
Wir haben mit jedem unserer Dienstleister für IT-Outsourcing bzw. Cloud Computing einen Vertrag geschlossen, der unsere definierten Anforderungen enthält und zu deren Erfüllung verpflichtet. *	○ Ja ○ Nein ○ Trifft auf unser Unternehmen nicht zu ○ Keine Angabe ?

* Feld muss ausgefüllt werden

Bemerkungen:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Analyse | Cyber-Quick-Check KMU

Vollmacht

Der Unterzeichner bevollmächtigt die atevis Aktiengesellschaft (kurz: atevis) auf der Grundlage obiger Angaben in dem Kundenfragebogen eine Ausschreibung für eine VSV/Cyber-Versicherung bei einer oder mehreren in Deutschland ansässigen und geeigneten Gesellschaften vorzunehmen.

Atevis ist bei der Auswahl der in Frage kommenden Gesellschaft(-en) frei, außer der Vollmachtgeber schließt eine oder mehrere Gesellschaften ausdrücklich von der Ausschreibung aus.

Gegenstand der Vollmacht ist die ausschließliche Vermittlung eines oder mehrerer Angebote.

Bei Abschluss eines durch atevis vermittelten Wareneinkaufsfinanzierungsvertrages wird eine Courtage fällig, die von der jeweiligen Gesellschaft an atevis gezahlt wird.

Die Vollmacht ist unbefristet und kann jederzeit ohne Einhaltung einer Frist schriftlich gekündigt werden. Bis zur Kündigung vermittelte Wareneinkaufsfinanzierer bleiben von der Kündigung unberührt.

Der Vollmachtgeber erklärt sich damit einverstanden, dass die obigen Angaben für die Kalkulation eines Angebotes dienen und - im Falle eines Vertragsabschlusses - Grundlage und Bestandteil des Vertrages werden.

Im Übrigen gelten die Allgemeinen Geschäftsbedingungen von atevis in ihrer jeweiligen Fassung. Sie sind auf den Webseiten unter www.atevis.de hinterlegt und können dort vom Vollmachtgeber eingesehen werden..

Ort: _____ Datum: _____

_____

Unterschrift | Firmenstempel