modelling advanced business security

Informationssicherheit Home-Office

Herausgeber

mabs4.0 Deutschland GmbH
Großenbaumer Weg 8
40472 Düsseldorf

Telefon: +49 211 205 444 80
Telefax: +49 211 205 444 81

Internet: http://mabs40.de.com

Vorwort

Liebe/r Leser/in,

herzlichen Dank für Ihr Interesse an unserem Portfolio.

Die **mabs4.0 Deutschland GmbH** aus Düsseldorf ist ein Beratungshaus mit dem spezifischen Fokus auf die drei Säulen **IT- & Informationssicherheit, Management-beratung und das Business Process Management**.

Als solches unterstützen wir erfolgreich unsere Kunden unter anderem bei der Umsetzung und Einführung von **Informationssicherheitsmanagementsystemen (ISMS) wie beispielsweise gemäß ISO27001, BSI Grundschutz oder TISAX®.**

Auch das parallele Management verschiedenster, meist ineinandergreifender Normen („Multi-Normen-Management“) kann dabei in den Mittelpunkt rücken.

Unser erfahrenes Team unterstützt Sie beratend als auch umsetzend mit nachgewiesener Expertise und langjährige Erfahrungen bei den für Sie notwendigen Ausarbeitungen und Anpassungen.

Unser Ziel ist es, unsere Kunden als Partner in Augenhöhe nach seinem tatsächlichen Bedarf zu unterstützen.

Unsere Leistungen orientieren sich immer nach der benötigten Angemessenheit und Wirtschaftlichkeit.

Kontaktieren Sie uns gerne und unverbindlich für ein erstes kostenloses Beratungsgespräch. Gerne kommen wir auch zu Ihnen und bewerten mit Ihnen Ihre Herausforderungen.

Herzliche Grüße

Eric Schneider
Geschäftsführer der mabs4.0 Deutschland GmbH

Inhalt

1 Über die mabs4.0 Deutschland GmbH

Die mabs4.0 Deutschland GmbH (kurz: mabs) ist ein international agierender und unabhängiger Düsseldorfer Spezialist für

- IT & Informationssicherheit,
- Integrierte Managementsysteme und
- Business Process Management.

Mit nachgewiesener Expertise behandelt die mabs die gesetzlichen und normativen Anforderungen zur Informationssicherheit, wie das deutsche IT-Sicherheitsgesetz oder die EU-DSGVO genauso wie Kunden- und Normanforderungen (z.B. TISAX® oder ISO27001) oder Maßnahmen der Digitalisierung (z.B. Cybersicherheit) und setzt diese erfolgreich gemeinsam mit Ihren Kunden um.

Die häufig hinzukommenden verschiedenen, teils bestehenden, Anforderungen aus Umweltschutz (z.B. ISO 14001), Qualitätsnormen (ISO 9001), Arbeitssicherheit (ISO 45001) oder weiterer Anforderungen können zudem in einem integrierten Managementsystem (IMS) erfasst werden.

Anhängige oder betroffene Prozesse und Strukturen werden durch unsere Experten bei Bedarf analysiert und modelliert.

mabs unterstützt seine Kunden aus den Branchen Automotive, Industrie & Maschinenbau, Dienstleistungen, Banking, Telekommunikation, Gesundheitswesen und Pharmazie in ihren Vorhaben mit Augenmaß und schafft so transparente Projektstrukturen und echten Kundennutzen:

• Etablierte Prozesse und Verantwortlichkeiten • Kostenminimierung • Nachweise der Erfüllung von Kundenanforderungen • Nachweis der Erfüllung von normativen und gesetzlichen Anforderungen • Haftungsreduzierung • Wettbewerbsvorteile • Minimierung von Risiken und möglichen Schäden

2 Home-Office

2.1 Was bedeutet eigentlich Home-Office?

Beim Home-Office handelt es sich in der Regel um die Verlagerung der betrieblichen Arbeit/Aufgaben in die häusliche private Umgebung. In Deutschland findet u. a. auch der Begriff Telearbeit oder Heimarbeit Anwendung. Der Mitarbeiter kommuniziert mit dem Unternehmen via E-Mail, Telefon oder über das firmeneigene Intranet. Das Home-Office kann sowohl von Mitarbeitern als auch von Selbstständigen genutzt werden.

Mitarbeiter, die im Home-Office arbeiten, bekommen hierfür die Arbeitsmittel vom Unternehmen gestellt. Dabei handelt es sich in der Regel um einen Laptop oder Computer sowie um weitere nötige Arbeitsmaterialien. Der Mitarbiter arbeitet entweder in der eigenen Wohnung oder an einem frei wählbaren geeigneten Arbeitsplatz außerhalb des Unternehmens.

2.2 Voraussetzungen für ein Home-Office

Home-Office wird meist angeboten, bzw. gewählt, um Mitarbeitern benötigte Flexibilität in Ihren geschäftlichen und privaten Alltag zu geben, bzw. in Ausnahmesituationen – beispielsweise der Cora-Krise, betriebliche Abläufe weiterhin aufrecht zu erhalten. Angesichts der möglichen IT- und Informationssicherheits-Risiken geben wir Ihnen nachfolgend ein paar wertvolle Hinweise, wie Sie als Unternehmen Ihre betrieblichen Risiken reduzieren können.

2.2.1 Regelung von Schutz der IT und Daten

Alle Mitarbeiter, die aus dem Home-Office an das Unternehmensnetzwerk angebunden sind, sollten verbindliche und eindeutige schriftliche Regelungen für den Schutz der bereitgestellten Hardware, der IT-Umgebung, der Daten und der Informationen des Unternehmens erhalten. Darüber hinaus sind geschulte Mitarbeiter der Beste und Erste Schutz vor Cyber-Angriffen oder Fehlverhalten.

2.2.2 Schutz von Endgeräten

Der aktuelle Informationsbedarf in der Corona-Krise wird verstärkt von Hackern ausgenutzt.

Über gefälschte Webseiten, E-Mails oder Grafiken, die aus scheinbar vertrauensvollen Quellen stammen, wird Schadsoftware auf die Rechner im Home-Office verteilt und kann so in das Unternehmensnetzwerk gelangen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt vor der Zunahme solcher Angriffe. Ein möglicher Schutz vor Angriffen aus dem Internet ist ein virtueller Browser, den das BSI im Rahmen der virtuellen Surfumgebung BitBox entwickeln ließ. Kommt dieser zum Einsatz, haben Cyber-Kriminelle keine Chance, bis zur Hardware des Rechners zu gelangen.

2.2.3 Schutz von Daten

Unternehmen mit hohen Sicherheitsanforderungen sollten die Endgeräte ihrer Mitarbeiter mit einer Festplattenverschlüsselung ausstatten. Nur berechtigte Nutzer können dann per Multi-Faktor-Authentifizierung ihre Daten und die entsprechenden Systeme / Programme nutzen. Geht das Gerät verloren oder wird es gestohlen, sollte es für Dritte unmöglich sein, auf die Daten zuzugreifen.

2.2.4 Deaktivierung USB Schnittstelle

Zusätzlich sollte die USB-Schnittstelle des Rechners durch die Administratoren per Gruppenrichtlinie für die Nutzung von externen Speichermedien deaktiviert werden, so dass eine Nutzung externer Datenträger erst gar nicht möglich ist. Hierdurch werden zwei Gefahrenszenarien minimiert: a) Schutz vor Schadsoftware (Viren, Trojaner, Würmer, Mal- und Spyware), b) Abfluss von Unternehmensdaten und Know-how.

2.2.5 Aktuelle Software

Egal ob Betriebssysteme, Web-Anwendungen oder Applikationen – alles muss auf dem aktuellsten Software-Stand (Patchlevel) des Anbieters sein. Dies ist ein wesentlicher Schutz vor Cyber Angriffen. Durch die Administration sollte dieser Aktualisierungsprozess automatisiert und die Unterbindung durch Mitarbeiter ausgeschlossen sein.

2.2.6 Sichere Kommunikation

Unternehmen sollten sichere Kommunikationskanäle nutzen, um die Endgeräte der Mitarbeiter im Home-Office an das Unternehmensnetz anzubinden. Empfehlenswert sind Virtual Private Networks (VPN). Sie bauen über einen "gesicherten Tunnel" eine Verbindung zwischen dem Endgerät und dem Unternehmensnetz auf.

2.2.7 Nutzung einer Cloud

Für das dezentrale Arbeiten sind Cloud-Anwendungen und Collaboration-Dienste ideal. Doch die Schutzmechanismen der Cloud-Anbieter entsprechen meist nicht den Sicherheitsanforderungen vieler Unternehmen. Es drohen Datenspionage und Compliance-Verletzungen. Die Lösung ist ein datenzentrischer Schutz: Dabei werden Platzhalter in die Cloud eingestellt, die nur Metadaten enthalten, die für Kollaboration und Workflows notwendig sind. Die schützenswerten Daten selbst werden dagegen fragmentiert im Unternehmensnetzwerk oder an einem anderen Ort abgelegt.

3 Regeln für ein sicheren Heimarbeitsplatz

3.1 Grundlegendes

Der Arbeitsplatz in den eigenen vier Wänden sollte physisch gesichert werden, indem Türen verschlossen und Bildschirme gesperrt werden. Empfehlenswert ist zudem, die Webcam am Rechner oder Laptop abzudecken, wenn diese nicht benötigt wird, sowie bei Nichtgebrauch das Mikrofon auszuschalten, um mögliche Spionageattacken ins Leere laufen zu lassen. Alexa, Siri und Google Home haben an einem Arbeitsplatz nichts zu suchen und sind entsprechend aus der unmittelbaren Nähe zu entfernen. Schriftliche Unterlagen sind bei Nichtnutzung gegen Zugriff durch Dritte, auch Mitgliedern des eigenen Haushaltes, zu schützen und sicher zu verstauen.

3.2 Sicheres WLAN

Grundsätzlich ist die heimische WLAN-Verbindung gegen Fremdnutzung abzusichern. Dazu ist das Standard-Administrator-Passwort durch ein neues, starkes Passwort zu ersetzen und mindestens die WPA2-Verschlüsselung zu aktivieren. Ein weiterer Schutz bietet der MAC-Adressen-Filter. Somit können nur bestimmte Geräte das heimische WLAN nutzen. Darüber hinaus muss der private Router auch mit der aktuellsten Herstellersoftware betrieben werden.

3.3 Vorsicht vor Betrügern

Angreifer täuschen und tricksen, um an Passwörter, Bankverbindungen oder Zugangsinformationen zu gelangen. Beispielsweise versenden sie täuschend echt wirkende E-Mails. Neben Phishing gilt aber auch Vorsicht bei Anrufen, SMS, Social-Media-Inhalten und gefälschten Nachrichten, die über Messenger verbreitet

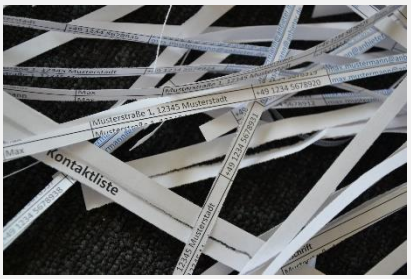
werden. Dieses sogenannte Social Engineering stellt in der jetzigen Zeit eines der größten Risiken im Home-Office dar.

3.4 Starke Passwörter

Passwörter schützen Anwendungen vor unberechtigtem Zugriff. Je komplexer und eindeutiger Passwörter sind, desto schwieriger sind sie zu knacken. Eine Multi-Faktor-Authentifizierung beispielsweise unter Einsatz von PIN, Fingerabdruck oder Passwort bietet ergänzend Schutz vor dem Zugriff unbefugter Dritter. Jede Anwendung sollte zudem mit einem eigenen Passwort geschützt werden. Andernfalls muss ein Angreifer lediglich eine Anwendung erfolgreich kompromittieren, um sich bei weiteren Konten erfolgreich anzumelden. Privat genutzte Passwörter dürfen nicht für geschäftliche Anwendungen verwendet werden.

3.5 Sichere Entsorgung von Informationen

Unternehmensbezogene Ausdrucke sollten keinesfalls direkt im privaten Papiermüll entsorgt werden. Empfehlenswert ist die Nutzung eines geeigneten Aktenvernichters. Nur so kann sichergestellt werden, dass unternehmensrelevante Daten nicht in privaten Mülltonnen gefunden werden können. Ist eine sichere Entsorgung im Home-Office nicht möglich, so sind papiergebundene Informationen zu sammeln und beim nächsten „Besuch“ im Unternehmen zu entsorgen.



4 Unser Portfolio

Wir haben nicht nur die Qualifikationen, sondern auch die fachliche Kompetenz und Praxiserfahrung. Unsere Kompetenz haben wir in vielen erfolgreichen Projekten unter Beweis gestellt. Alle von uns unterstützten Unternehmen sind erfolgreich unabhängig zertifiziert worden und verfügen über ein etabliertes Informationssicherheitsmanagementsystem (ISMS).

Engagement, Know-how und Zuverlässigkeit: Das ist unser Erfolgsrezept. Wir arbeiten konsequent an unseren Kompetenzen und unserer Qualität, damit unsere Kunden ihre Ziele erreichen und Ihr Geschäft zukunftssicher entwickeln. Wir arbeiten mit Leidenschaft an den Projekten unserer Kunden.

Wir haben das Ziel unsere Kunden zu begeistern und bauen auf eine langfristige Partnerschaft. Durch engagiertes und verantwortungsvolles Handeln eines jeden Einzelnen erreichen wir ein Höchstmaß an Identifizierung mit unseren Kunden.

Unser Portfolio für Sie:

- Kostenlose Erstberatung zur IT- & Informationssicherheit
- Vor Ort Bewertung Ihrer IT- & Informationssicherheit
- GAP-Analysen
- Projektierung zur Einführung von IT- & Informationssicherheitsmanagementsystemen
- Integration von bestehenden Managementsystemen
- Risikobewertungen
- Business Impact Analysen
- Erstellung von Richtlinien und Verfahrensanweisungen
- Prozess-Analyse, -darstellung, -optimierung und Digitalisierung
- Schulungen von Mitarbeitern
- Begleitung zur Zertifizierung gemäß ISO/IEC 27001, BSI Grundschutz und TISAX®

Kontakt

mabs4.0 Deutschland GmbH
Großenbaumer Weg 8
40472 Düsseldorf

Telefon: +49 211 205 444 80
Telefax: +49 211 205 444 81

E-Mail: kontakt@mabs40.com
Internet: http://mabs40.de.com