Datensicherheit

1. Jedes Sicherheitsleck kann das Unternehmensimage schädigen und Sicherheitsvorfälle können ein Unternehmen ruinieren.
2. Cyberangriffe können verheerende Folgen haben, wie im Fall des Hackerangriffs auf Kaseya, bei dem eine Erpressungssoftware in 17 Ländern entdeckt wurde und eine Lebensmittelkette hunderte Filialen schließen musste. - Argumentationskraft
3. Cyber-Diebstahl, Spionage und Sabotage verursachen der deutschen Wirtschaft jährlich einen Schaden von rund 223 Milliarden Euro.
4. Sensibilisierung der Mitarbeiter, Erkennung von Angriffsmöglichkeiten und Bereitschaft für Notfallmaßnahmen sind wichtig.
5. Der Staat hat strenge Gesetze erlassen, die Unternehmen zur Gewährleistung der IT-Sicherheit verpflichten.
6. Die IT Sol GmbH strebt eine Zertifizierung nach ISO 27001 im Rahmen des BSI-Grundschutzes an.
7. Das BSI bietet eine Sicherheitsleitlinie und erfordert die systematische Erarbeitung eines Sicherheitskonzepts.
8. Es sind technische und organisatorische Maßnahmen (TOM) zu ergreifen, z. B.
   * physische Absicherung
   * Netzwerksicherheit,
   * Umgang mit klassifizierten Informationen,
   * Identitäts- und Berechtigungsmanagement,
   * Kryptografie,
   * Datensicherung
   * Schadsoftwareerkennung/-abwehr.
9. Unternehmen sind verpflichtet, angemessene Informationssicherheitssysteme einzuführen, insbesondere wenn sie personenbezogene Daten verarbeiten, gemäß der Datenschutzgrundverordnung (DSGVO).

Schutzziele

Die drei primären Schutzziele sind:

* + Vertraulichkeit
  + Integrität
  + Verfügbarkeit

Vertraulichkeit:

bezieht sich auf den Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten sollten nur befugten Personen zugänglich sein

Integrität:

bezeichnet die Sicherstellung der Korrektheit und Unversehrtheit von Daten und Systemen. Informationen dürfen nicht unerlaubt verändert oder manipuliert werden

Verfügbarkeit:

bedeutet, dass Dienstleistungen, Funktionen, Anwendungen und Informationen stets wie vorgesehen genutzt werden können.

Es gibt außerdem noch weitere Schutzziele, welche berücksichtigt werden müssen:

Authentizität:

gewährleistet, dass die Kommunikationspartner und Informationen tatsächlich diejenigen sind, für die sie sich ausgeben.

Nichtabstreitbarkeit:

bezieht sich auf den Nachweis gegenüber Dritten, dass Daten gesendet oder empfangen wurden, ohne dass diese in Abrede gestellt werden können.

Verbindlichkeit:

kombiniert die Sicherheitsziele Authentizität und Nichtabstreitbarkeit, um sicherzustellen, dass die Identität der Informationsquelle bewiesen ist und der Empfang nicht abgestritten werden kann.

Zulässigkeit:

bezieht sich auf die technische Funktionsfähigkeit von IT-Systemen und Komponenten.

Ein Grundprinzip der Datensicherheit ist das „VIVA“-Prinzip. Dieses umfasst die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität.

Checkliste um die Informationssicherheit zu erhöhen

1. Bewusstsein schaffen
2. Identifizierung von Informationswerten und Geschäftsprozessen
3. Strategieentwicklung
4. Ganzheitliches Managementsystem
5. Sensibilisierung und Schulung
6. Zugriffsrechte und Berechtigungen verwalten
7. Sicherheitsmaßnahmen implementieren
8. Incident-Response-Plan
9. Externe Audits und Penetrationstests
10. Datenschutz-Compliance

DSVGO

Die Datenschutz-Grundverordnung (DSGVO) ist eine europäische Datenschutzgesetzgebung, die den Schutz personenbezogener Daten regelt und einheitliche Standards für den Umgang mit personenbezogenen Daten in der EU festlegt. Sie legt Rechte und Pflichten für Unternehmen, Organisationen und Behörden fest, um die Privatsphäre und den Datenschutz von EU-Bürgern zu gewährleisten.

Recht auf Auskunft:

Personen haben das Recht, von einer Organisation Auskunft darüber zu verlangen, ob und welche personenbezogenen Daten von ihnen verarbeitet werden. Dies umfasst Informationen über den Verarbeitungszweck, die Kategorien der verarbeiteten Daten, die Empfänger der Daten und die geplante Speicherdauer. Die Organisation muss die angeforderten Informationen in einer klaren und verständlichen Weise bereitstellen.

Recht auf Berichtigung:

Wenn eine Person feststellt, dass ihre personenbezogenen Daten unrichtig oder unvollständig sind, hat sie das Recht, von der verantwortlichen Organisation eine Berichtigung oder Ergänzung dieser Daten zu verlangen. Die Organisation ist verpflichtet, die Daten zu aktualisieren und sicherzustellen, dass sie korrekt sind.

Recht auf Löschung:

Personen haben unter bestimmten Bedingungen das Recht, von einer Organisation die Löschung ihrer personenbezogenen Daten zu verlangen. Dies kann zum Beispiel der Fall sein, wenn die Daten nicht mehr für den ursprünglichen Verarbeitungszweck benötigt werden, die Einwilligung widerrufen wurde oder die Daten unrechtmäßig verarbeitet wurden. Die Organisation muss die Daten innerhalb einer angemessenen Frist löschen, es sei denn, es bestehen rechtliche Gründe oder legitime Interessen, die der Löschung entgegenstehen.

Das deutsche Gegenstück zur DSVGO ist das Bundesdatenschutzgesetz (BDSG). Es ergänzt und konkretisiert die Bestimmungen der DSGVO und enthält spezifische Regelungen für den Datenschutz in Deutschland. Das BDSG dient der Umsetzung und Anwendung der DSGVO auf nationaler Ebene und legt zusätzliche Vorschriften und Regelungen fest, die für den Datenschutz in Deutschland gelten.

Welche zwei organisatorischen Einheiten kümmern sich um die Implemetierung eines Sicherheitskonzepts in einem Unternehmen?

* + IT-Sicherheitsbeauftragte (ISB)
  + Datenschutzbeauftragte (DSB)

Welche Maßnahmen können ergriffen werden, um die Datensicherheit für Privatpersonen und Mitarbeiter eines Unternehmens zu gewährleisten?

1. Regelmäßige Sicherheitsupdates
2. Virenschutzprogramme
3. Keine E-Mails von unbekanntem Absender öffnen
4. Regelmäßige Datensicherungen
5. Passwörter verwenden
6. VPN
7. Bildschirme so positionieren, dass sie von keinem Fenster eingesehen werden können
8. Nur gesicherte USB-Sticks verwenden

Welche zusätzlichen Maßnahmen muss ein Unternehmen implementieren?

1. Regelmäßige Backups
2. Verschlüsselte Datenübertragung
3. Firewalls einsetzen
4. Rechteverwaltung
5. Datenänderungen nachvollziehbar machen
6. Zutritt zu Räumen regeln
7. Prozesse dokumentieren
8. Datensicherheitsbeauftragten einsetzen
9. Eine Schutzbedarfsanalyse durchführen bzw. durchführen lassen

Schutzbedarfsanalyse – Durchführung

1. Bestandsaufnahme: Es wird ermittelt, welche Arten von Informationen und Daten in der Organisation vorhanden sind, wie sie verarbeitet werden und welche Systeme und Infrastrukturen dafür verwendet werden.
2. Bedrohungsanalyse: Es werden potenzielle Bedrohungen und Gefahren identifiziert, die die Vertraulichkeit, Integrität oder Verfügbarkeit der Informationen beeinträchtigen könnten. Dazu gehören z.B. Cyberangriffe, physische Diebstähle oder menschliches Fehlverhalten.
3. Risikobewertung: Die identifizierten Bedrohungen werden hinsichtlich ihrer Eintrittswahrscheinlichkeit und ihres potenziellen Schadens bewertet. Dadurch werden die Risiken für die Informationssicherheit quantifiziert.
4. Schutzbedarfsermittlung: Auf Basis der Risikobewertung wird der Schutzbedarf für die einzelnen Informationen und Daten festgelegt. Dabei werden Kriterien wie Vertraulichkeit, Integrität, Verfügbarkeit, Rechtskonformität und wirtschaftlicher Wert berücksichtigt.
5. Maßnahmenfestlegung: Es werden die geeigneten Sicherheitsmaßnahmen und Kontrollen bestimmt, um den ermittelten Schutzbedarf zu erfüllen. Dies können technische, organisatorische oder rechtliche Maßnahmen sein, wie z.B. Verschlüsselung, Zugriffskontrollen, Schulungen oder Datenschutzrichtlinien.
6. Umsetzung und Überwachung: Die definierten Maßnahmen werden implementiert und regelmäßig überwacht, um sicherzustellen, dass der ermittelte Schutzbedarf weiterhin erfüllt wird. Bei Veränderungen in der Organisation oder neuen Bedrohungen sollte die Schutzbedarfsanalyse regelmäßig aktualisiert werden.