DIGITALE GEHEIMNISSE:
DEINE DATEN, DEINE SICHERHEIT

KUPPER Gruppe.

1. IST-ANALYSE

WAS?
Was sind denn meine schützenswerten Daten? Was wollen wir eigentlich schützen? z.B. Finanzinformationen, Kundendaten in einer Kundendatenbank, Unternehmens-Know-how, Patentente, sensible Geschäftsprozesse

WO?
Wo sind meine sensiblen Daten gespeichert?

WER?
Wer hat Zugriff auf diese Informationen?

WIE?
Wie wird mit den Daten umgegangen?

2. DATENKLASSIFIZIERUNG VORNEHMEN

- Daten anhand ihres Schutzbedarfs bewerten
- Welche Daten sind mehr oder weniger schützenswert?
- Klassifizierungskategorien können sein:
  - öffentlich
  - vertraulich
  - sensibel
  - personenbezogen

3. ORGANISATORISCHE UND TECHNISCHE MASSNAHMEN ERGREIFEN

ORGANISATORISCHE MASSNAHMEN

- Zugriffs- und Rechtekonzepte nach dem Least-Privilege-Prinzip erstellen
- Rechte, Regeln & Konzepte für die Vernichtung von Daten erstellen
- Eventuelle Geheimhaltungsvereinbarungen abschließen

Good to know!

Was ist das LEAST-PRIVILEGE-PRINZIP?

Man erlangt nur so viele Informationen und Zugriffsrechte, die man auch zwingend für seine Tätigkeit braucht.

TECHNISCHE MASSNAHMEN

- Datenverschlüsselung vornehmen
  1. Transportverschlüsselung einrichten
  2. Daten auf Datenträgern schützen (z.B. Festplattenverschlüsselung, Backup- und Disaster-Recovery-Strategien)

SAFER SEC

DER IT-SICHERHEITS-PODCAST FÜR UNTERNEHMEN UND DIE ÖFFENTLICHE VERWALTUNG.

Unsere Security-Experten erreicht ihr hier:

it-security@kupper-it.com

NICHT VERGESSEN & ABONNIEREN!

Anhören auf Spotify | Anhören auf Apple Podcast | Anhören auf Google Podcast
Anhören auf Amazon Music | Anhören auf Deezer | Anhören auf YouTube Music

KUPPER
IT. innovativ. effizient. sicher.

KUPPER Gruppe.

DIGITALE GEHEIMNISSE: DEINE DATEN, DEINE SICHERHEIT

4. NOTFALLMANAGEMENT ETABLIEREN

- Im Falle einer Datenpanne Panik vermeiden und nicht unbedacht agieren
- Stattdessen schnell und organisiert handeln
- Wichtige Schritte im Notfallmanagement:
  - Ursache herausfinden
  - Verursachten Schaden einschätzen
  - Auswirkungen evaluieren
  - Eventuelle Meldepflichten einhalten
  - Learnings für die Zukunft ableiten
  - Vorfall transparent an die Mitarbeiter kommunizieren

5. PRÄVENTIVE MASSNAHMEN EINFÜHREN

- In regelmäßigen Abständen Ist-Analysen durchführen und Maßnahmen dementsprechend anpassen
- Systeme und Anwendungen immer auf einem aktuellen Stand halten (Firmware, Updates, Patches, aktuelle Hard- & Software)
- Regelmäßig Mitarbeiter- und Managementschulungen veranstalten

Wichtig Sicherheit & Awareness müssen von der Führung vorgelebt werden!

SAFER SEC VORSCHAU

DIE THEMEN UNSERER NÄCHSTEN FOLGEN

Folge 5, 14.11.
Authentifizierung (Zugriffskonzepte)
- Passwörter & Multifaktor-Authentifizierung
- Erweiterte Authentifizierungskonzepte
- Zero Trust Ansatz

Folge 6, 28.11.
Netzwerksegmentierung & WLAN
- Warum Netzwerksegmentierung wichtig ist
- Unterschiedliche WLANs im Unternehmen
- Internet of Things

Folge 7, 12.12.
Patchmanagement & Updates
- Warum neu nicht immer besser ist
- Warum alt aber definitiv immer schlecht ist
- Konzepte für die goldene Mitte

Folge 8, 02.01.
Datensicherung (Backups)
- 3-2-1-Regel
- Unveränderliche Backups (Immutable Backups)
- Disaster Recovery

Folge 9, 16.01.
Notfallmanagement
- Organisation vs. Technik
- Sofortmaßnahmen
- Folgemaßnahmen
- Externe Hilfe

KUPPER
IT. innovativ. effizient. sicher.