Ihre Informationssicherheit.

Was jetzt zu tun ist.

Ein kleines Kochrezept.

3 Erkenntnisse des Tages: Sie. Sind. Verantwortlich!

- Wer trägt die Verantwortung für die Informationssicherheit?
  - Der Administrator? NEIN!
  - Der externe Dienstleister? NEIN!
  - Der IT-Leiter? NEIN!
  - Der Datenschutzbeauftragte? NEIN!
- Sie (und nur Sie) als Geschäftsführung sind verantwortlich.
  - Nehmen Sie Ihre Verantwortung wahr.
  - Kümmern Sie sich! (Keine Angst – es ist kein Hexenwerk!)
  - Alles andere ist grob fahrlässig.

Datensicherung, Datensicherung, Datensicherung, Datensicherung!!!

- Daten können unbrauchbar werden oder verloren gehen. Deshalb ist es notwendig, durch eine Datensicherung die Integrität und Verfügbarkeit ihrer Unternehmensdaten sicherzustellen:
  - Legen Sie als Geschäftsführung jene Orte fest, an denen Ihre Mitarbeiter Daten speichern dürfen (verbindliche Richtlinie).
  - Lassen Sie Ihre Administratoren/Dienstleister die Vorgehensweisen für die Datensicherung und -wiederherstellung der Speicherorte definieren und dokumentieren.
  - Legen Sie die Intervalle der Datensicherungen fest. Empfehlung: Speicherorte müssen so gesichert werden, dass ihr letzter vollständig wiederherstellbarer Zustand nicht älter als 24 Stunden ist.
  - Lassen Sie die gesicherten Daten nicht im gleichen Brandabschnitt wie die gesicherten IT-Systeme aufbewahren.
  - Fordern Sie, dass einmal jährlich ein gesichertes IT-System nach dem Zufallsprinzip ausgewählt und in einer Testumgebung wiederhergestellt wird. Die Tests sollten ohne Unterstützung durch den jeweiligen Verantwortlichen für die Datensicherung erfolgen. Vielmehr sollten sie von einem anderen Mitarbeiter anhand der vorliegenden Dokumentation bewältigt werden.

Effektiv und effizient: Verantwortlichkeiten definieren!

- Die größte Schwachstelle sitzt 50cm vor dem Bildschirm. Mitarbeiter benötigen klare Regeln, was in der IT erlaubt und was definitiv verboten ist:
  - Untersagen Sie das unrechtmäßige Abrufen oder Verbreiten von Inhalten, die urheberrechtlich geschützt, strafrechtlich relevant oder sittenwidrig sind.
  - Legen Sie fest, ob die private Nutzung der IT erlaubt ist und gestalten Sie die Privatnutzung nach den Bedürfnissen des Unternehmens aus.
  - Bestimmen Sie, dass nur freigegebene Hard- und Software in der IT-Infrastruktur installiert, genutzt oder betrieben wird.
  - Untersagen Sie, die in der IT-Infrastruktur installierten Sicherheitseinrichtungen zu deinstallieren, zu deaktivieren, mutwillig zu umgehen oder in ihrer Konfiguration zu verändern.
  - Regeln Sie, ob und wann auf den Datenbestand von abwesenden Mitarbeitern zugegriffen werden darf.

Der Schlüssel zu Ihrem digitalen Werten: Mitarbeiter, Zugänge, Zugriffsrechte

- Mitarbeiter, Zugänge und Zugriffsrechte erlauben es, auf ihre nichtöffentliche IT und ihre Informationen zuzugreifen. Eine strukturierte Verwaltung ist hier unbedingt notwendig:
  - Legen Sie fest, dass im Rahmen ihrer Einarbeitung neue Mitarbeiter in die Regelungen der Informationssicherheit eingewiesen werden müssen.
  - Legen Sie fest, dass bei Beendigung oder Wechsel einer Anstellung die Zugänge und Zugriffsrechte des Mitarbeiters umgehend überprüft und bei Bedarf angepasst werden.
  - Legen Sie fest, dass Mitarbeiter nur jene Zugänge und Zugangsrechte erhalten, die sie für ihre Aufgabenerfüllung benötigen (Schreib- und Leserechte für alle auf alle Daten des Unternehmens ist keine gute Idee).
  - Schreiben Sie vor, dass Zugriffe auf nichtöffentliche Bereiche Ihrer IT durch geeignete Anmeldeverfahren abgesichert werden müssen, die eine Authentifizierung verlangen.

Härten Ihrer IT: Basisschutz für alle IT-Systeme

- Sämtliche IT-Systeme müssen über ein Mindestmaß an technischen Sicherheitsmaßnahmen verfügen. Lassen Sie mindestens folgende Punkte von ihren Administratoren sicherstellen:
  - Verfügbare Sicherheitsupdates für die System- und Anwendungssoftware müssen installiert werden.
  - IT-Systeme müssen gekapselt werden, wenn sie über Schwachstellen verfügen, die nicht behoben werden (z. B. wenn keine Sicherheitsupdates installiert werden können, Passwörter nicht geändert werden können oder unsichere technische Verfahren eingesetzt werden).
  - An- und Abmelden von Nutzern, Fehler und Informationssicherheitsereignisse müssen protokolliert werden.
  - Die Windows-Systeme werden mit einer Anti-Viren-Software geschützt.
  - Normale Nutzer arbeiten nicht mit Administratorrechten.

Innovative Technologien: Black Box?

- Die Informationstechnologie entwickelt sich rasant. Dabei werden Sicherheitsbedürfnisse von den Herstellern häufig nicht wahrgenommen oder als hinderlich empfunden. Hier ist Nachfragen und der gesunde Menschenverstand gefragt. Fragen Sie die Hersteller oder den Händler!
  - Wie stellen Sie sicher, dass Nutzer ausreichend authentifiziert werden?
  - Wie stellen Sie sicher, dass übertragene Daten vertaulich sind?
  - Können Updates eingespielt werden?
  - Wie erhalte ich Informationen über sicherheitskritische Updates?
  - Wie lange habe ich Support?

(Fast) zum Schluss: Ein paar offene Worte

- Die Maßnahmen der letzten Seiten stellen ein absolutes Mindestmaß dar. Viele wichtige Bereiche (wie z. B. der Umgang mit Smartphones, USB-Sticks oder Cloud-Computing) sind nicht erfasst.
- Durch die Maßnahmen der letzten Seiten arbeiten Sie zumindest nicht mehr grob fahrlässig. Sie besitzen aber dennoch ein erhebliches Restrisiko.
- Hier gilt:
  Risiken, die Sie nicht beherrschen sollten Sie abwälzen!

Versichern Sie Ihre IT bei der VHV!

Weitere Infos: VdS 3473

- Alle Maßnahmen dieses Papiers sind aus der VdS Richtlinie 3473 entnommen.
- Die VdS-Richtlinien 3473 definieren Mindestanforderungen an die Informationssicherheit und sind speziell auf KMU zugeschnitten. Sie bieten genau das Schutzniveau, das kleine und mittlere Unternehmen benötigen, ohne sie finanziell oder organisatorisch zu überfordern.

VdS 3473: hier kostenfrei verfügbar

http://vds.de/fileadmin/vds_publikationen/vds_3473_web.pdf

Umsetzungshilfen verfügbar

- Webseite mit umfangreichen Hilfestellungen für die Implementierung:
  - ausführliche Kommentierung der Maßnahmen und Empfehlungen
  - Vorlagen für die Erstellung der Leitlinie, der Richtlinien und Verfahren
  - Hintergrundartikeln z. B. zu Risikoanalysen und Konzepten
  - Empfehlungen für die Vorgehensweise und das Projektmanagement

https://www.3473-wiki.de