Ihre Informationssicherheit.

WAS SIE DEFINITIV TUN SOLLTEN.

MINDESTENS.

Ein kleines Kochrezept.

Mark Semmler

WIE HEUTE LEIDER (VIEL ZU) VIELE UNTERNEHMEN AUSSEHEN...

WER IST FÜR DIE IT VERANTWORTLICH?

- Sie als Geschäftsführung müssen nicht im Detail verstehen, wie die IT funktioniert. Dafür gibt es Spezialisten.
- Sie sollten aber festlegen, welche Anforderungen die IT zu erfüllen hat (die IT ist ein Betriebsmittel).
- Auf den folgenden Slides finden Sie eine Aufstellung der wichtigsten Dinge, die Sie im Unternehmen geregelt haben sollten.
- Anmerkung:
  Der Königsweg für Informationssicherheit nach dem Prinzip „So viel wie nötig, so wenig wie möglich!“ ist die Installation eines ISMS (Informationssicherheitsmanagementsystem).
  Ein ISMS sorgt dafür, dass die notwendige Informationssicherheit definiert, umgesetzt und fortlaufend angepasst/verbessert wird.

DATENSICHERUNG. DATENSICHERUNG! DATENSICHERUNG!! DATENSICHERUNG!!!

- Daten können unbrauchbar werden oder verloren gehen.
- Deshalb muss Ihr Unternehmen über eine strukturierte Datensicherung verfügen!
  - » Legen Sie in einer verbindlichen Richtlinie die Orte fest, an denen Ihre Mitarbeiter Daten speichern dürfen (definieren Sie die Speicherorte).
  - » Lassen Sie Ihre Administratoren/Dienstleister die Vorgehensweisen für die Datensicherung und -wiederherstellung der Speicherorte ausarbeiten 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 anhand der vorliegenden Dokumentation bewältigt werden (siehe oben).

EFFEKTIV UND EFFIZIENT: VERANTWORTLICHKEITEN DEFINIEREN!

- Die größte Schwachstelle sitzt ca. 50cm vor dem Bildschirm.
- Mitarbeiter benötigen klare Regeln, was in der IT erlaubt und was 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. Wenn Sie die private Nutzung erlauben, so gestalten Sie sie gemäß der 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.

DIE 3 SCHLÜSSEL ZU IHREN 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 die folgendes fest:
  - » Im Rahmen der Einarbeitung werden neue Mitarbeiter in die Regelungen der Informationssicherheit eingewiesen.
  - » Bei Beendigung oder Wechsel einer Anstellung werden die Zugänge und Zugriffsrechte des Mitarbeiters umgehend überprüft und bei Bedarf angepasst.
  - » Mitarbeiter erhalten nur jene Zugänge und Zugangsrechte, die sie für ihre Aufgabenerfüllung benötigen.
  - » Zugriffe auf nichtöffentliche Bereiche der IT werden durch geeignete Anmeldeverfahren abgesichert, die eine Authentifizierung verlangen.

WERDEN SIE ZUM STAHLWOLLSCHAF: BASISSCHUTZ FÜR ALLE IT-SYSTEME!

- IT-Systeme müssen über ein Mindestmaß an Sicherheitsmaßnahmen verfügen.
- Lassen Sie mindestens folgende Punkte von ihren Administratoren bzw. von Ihrem Dienstleister sicherstellen:
  - » Verfügbare Sicherheitsupdates für System- und Anwendungssoftware werden installiert (Details wie Häufigkeit, Tests, Freigaben und Ausnahmen werden individuell auf Ihre IT abgestimmt).
  - » IT-Systeme werden gekapselt, 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 werden protokolliert.
  - » Windows-Systeme werden durch eine Anti-Viren-Software geschützt.
  - » Normale Nutzer arbeiten nicht mit Administratorrechten.

NEUE TECHNOLOGIEN: MIT EINFACHEN FRAGEN ZUR KERNBOHRUNG

- Die Informationstechnologie entwickelt sich rasant. Dabei werden Sicherheitsbedürfnisse von den Herstellern häufig nicht wahrgenommen oder als hinderlich empfunden.
- Wenn eine neue Technologie angeschafft/eingesetzt werden soll, können Sie ohne Vorwissen jeden Hersteller/Händler/Administratoren mit einfachen Fragen aus der Reserve locken (achten Sie im Gespräch auf die Gesichtsfarbe Ihres Gegenübers):
  - » Gibt es ein Sicherheitskonzept in dem mögliche Angriffe und die getroffenen Gegenmaßnahmen aufgeführt sind?
  - » Können Updates eingespielt werden?
  - » Wie erhalte ich von Ihnen Informationen über Updates?
  - » Wie lange habe ich Support?

(FAST) ZUM SCHLUSS: EIN PAAR OFFENE WORTE

- Die Maßnahmen der letzten Seiten stellen ein absolutes Mindestmaß dar. Viele 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 völlig ungeschützt. Sie besitzen aber ggf. noch ein (erhebliches) Restrisiko…
- Nicht beherrschbare Risiken kann man abwälzen.
  Denken Sie auch über eine Versicherung nach.

EPILOG

Weitergehende Infos.

VDS QUICK CHECK: EINE KURZE STANDORTBESTIMMUNG FÜR KMU

- Wo stehen Sie? Wie gut ist Ihr Unternehmen aufgestellt? Was müssen Sie noch tun?
- Verschaffen Sie sich einen Überblick in 15 bis 20 Minuten.
- Kostenfrei und auf Wunsch auch anonym.
- Klare und transparente Ergebnisse, umgehend geliefert.
- Drei Quick Checks stehen bereit:
  - Informationssicherheit
  - Informationssicherheit für Industrieanlagen (Industrial Control Systems – ICS)
  - EU Datenschutzgrundverordnung (EU-DSGVO)

https://www.vds-quick-check.de

SOLIDER RUNDUMSCHUTZ FÜR KMU: DIE VDS-RICHTLINIE 10000

- Alle Maßnahmen der letzten Slides stammen aus der VdS Richtlinie 10000 entnommen (kurz: VdS 10000).
- Die VdS 10000 definiert Mindestanforderungen an die Informationssicherheit und sind speziell auf KMU zugeschnitten.
- Sie bietet genau das Schutzniveau, das kleine und mittlere Unternehmen benötigen, ohne sie finanziell oder organisatorisch zu überfordern.
- Die VdS 10000 ist kostenfrei verfügbar.

https://vds.de/cyber/

VDS 10000: UMSETZUNGSHILFEN VERFÜGBAR

- Sie müssen das Rad nicht neu erfinden, wenn Sie die VdS 10000 (ganz oder in Teilen) umsetzen möchten
- Es gibt eine Webseite mit umfangreichen Hilfestellungen für die Implementierung:
  - » ausführliche Kommentierung der Maßnahmen und Empfehlungen
  - » Vorlagen für die benötigten Dokumente
  - » Hintergrundartikel
  - » Empfehlungen zur Vorgehensweise für die Umsetzung der VdS 10000

3473 Wiki

https://www.3473-wiki.de/

UMSETZUNG DER EU-DSGVO EINFACH GEMACHT: DIE VDS-RICHTLINIE 10010

- Die EU-Datenschutzgrundverordnung ist im Mai 2018 nach einer zweijährigen Übergangsfrist in Kraft getreten.
- Die VdS-Richtlinie 10010 (gesprochen: VdS zehn-null-zehn) zeigt, was zu tun ist.
- Informationssicherheit und Datenschutz gehen Hand in Hand. Deshalb sind die VdS 10010 und die VdS 10000 in vielen Anforderungen deckungsgleich, was die Umsetzung beider Richtlinien vereinfacht.
- Auch die VdS 10010 ist kostenfrei verfügbar.

https://vds.de/cyber/

BEI FRAGEN:

Mark Semmler

sicherheit [at] mark [minus] semmler [punkt] de

+49 163 7327475