

Nachlese der VHV Bautage 2018:

Ihre Informationssicherheit.

**WAS JETZT ZU TUN IST.  
MINDESTENS.**

Ein kleines Kochrezept.

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



VHV Bautage – Kochrezept – Version 180320 – [Klassifizierung:öffentlich] – Folie 2

Mark Semmler

# DIE DREI 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 eine strukturierte Datensicherung absolut notwendig!

- » Legen Sie in einer verbindlichen Richtlinie die Orte fest, an denen Ihre Mitarbeiter Daten speichern dürfen (Speicherorte).
- » 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 anhand der vorliegenden Dokumentation bewältigt werden (siehe oben).

# EFFEKTIV UND EFFIZIENT: VERANTWORTLICHKEITEN DEFINIEREN!

- Die größte Schwachstelle sitzt 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 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.

# 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

- Sämtliche IT-Systeme müssen über ein Mindestmaß an Sicherheitsmaßnahmen verfügen. Lassen Sie mindestens folgende Punkte von ihren Administratoren sicherstellen:
  - » Verfügbare Sicherheitsupdates für System- und Anwendungssoftware werden installiert.
  - » 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. Hier ist Nachfragen und der gesunde Menschenverstand gefragt.
- Fragen Sie die Hersteller oder den Händler folgende Fragen (und achten Sie dabei auf die Gesichtsfarbe Ihres Gegenübers):
  - » Wie stellen Sie sicher, dass Nutzer ausreichend authentifiziert werden?
  - » Wie stellen Sie sicher, dass übertragene Daten vertraulich 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 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...

**NICHT  
BEHERRSCHBARE  
RISIKEN KANN  
MAN ABWÄLZEN.**

**DENKEN SIE  
ÜBER EINE  
VERSICHERUNG  
NACH.**

# SOLIDER RUNDUMSCHUTZ FÜR KMU: DIE VdS-RICHTLINIE 3473

- Alle Maßnahmen dieses Papiers sind aus der VdS Richtlinie 3473 entnommen.
- Die VdS-Richtlinie 3473 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 3473 ist kostenfrei verfügbar.



[http://vds.de/fileadmin/vds\\_publicationen/vds\\_3473\\_web.pdf](http://vds.de/fileadmin/vds_publicationen/vds_3473_web.pdf)

# VDS 3473: UMSETZUNGSHILFEN VERFÜGBAR

- Webseite mit umfangreichen Hilfestellungen für die Implementierung:
  - » ausführliche Kommentierung der Maßnahmen und Empfehlungen
  - » Vorlagen für alle benötigten Dokumente
  - » Hintergrundartikel z. B. zu Risikoanalysen und Konzepten
  - » Empfehlungen zur Vorgehensweise und das rund um das Projektmanagement für die Umsetzung der VdS 3473



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

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

- Die EU-Datenschutzgrundverordnung tritt im Mai 2018 nach einer zweijährigen Übergangsfrist in Kraft.
- 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 3473 in vielen Anforderungen deckungsgleich, was die Umsetzung beider Richtlinien vereinfacht.
- Die VdS 10010 ist kostenfrei verfügbar.



[https://vds.de/fileadmin/vds\\_publicationen/vds\\_10010\\_web.pdf](https://vds.de/fileadmin/vds_publicationen/vds_10010_web.pdf)

# 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>