Eine Stunde Datenschutz

NIS2:
Neue Richtlinie zur Sicherheit von Netz- und Informationssystemen

Eine Stunde Datenschutz

- Webinar-Reihe des Arbeitskreises Datenschutz sowie des Servicezentrums, Team Rechtsservice, der Wirtschaftskammer Kärnten
- Vortragende:

  Mag. Günther Zikulnig

  Mag.a Judith Leschanz

  Ing. Günther Bauer

  Ing. Walter Wratschko
- Moderation:

  Dr. Christina Kitz-Überall

Eine Stunde Datenschutz

Sicherheit durch Technik – TOMs einfach erklärt

- DDSB.AT Beratung GmbH I **T** +43 (0)1/420 00 50 50 I **E** guenther.zikulnig@ddsb.at **I** **W** www.ddsb.at I Sorgogasse 10/32, 1130 Wien
  Zikulnig Consulting I **T** +43 (0)664/819 33 35 I **E** office@zikulnig.at **I** **W** www.zikulnig.at I Klagenfurter Straße 9, 9100 Völkermarkt
- Mag.a Judith Leschanz I Geschäftsführerin Data Betriebsberatungs - Gesellschaft m.b.H. I **T** +43 (0)1/533 4207-0 I **E** office@secur-data.at I **W** http://www.secur-data.at/ I Fischerstiege 9, 1010 Wien
- Ing. Günther Bauer, AFM Solutions GmbH I **T** +43 (0)664/133 23 90 I **E** bauer@afm-solutions.at I **W** www.afm-solutions.at I Adi-Dassler-Gasse 2/1, 9073 Klagenfurt
- Ing. Walter Wratschko I **T** +43 (0)699/15 04 38 60 I **E** walter.wratschko@datenschutz-sued.at I **W** www.datenschutz-sued.at I Office Klagenfurt: Brunnplatz 5, 9020 Klagenfurt, Office Wien: Esteplatz 3, 1030 Wien

- https://www.wko.at/branchen/k/information-consulting/unternehmensberatung-buchhaltung-informationstechnologie/arbeitskreis-datenschutzexperten.html
- Dr. Christina Kitz-Überall, Servicezentrum, Rechtsservice, Wirtschaftskammer Kärnten **T** 05 90 90 4 – 723 I **E** christina.kitz-ueberall@wkk.or.at

Ein Stunde Datenschutz

Sicherheit durch Technik - NIS2: „Neue Richtlinie zur Sicherheit von Netz- und Informationssystemen"

Mag. iur. Günther Zikulnig

DDSB.AT
DATENSCHUTZ & DIGITALISIERUNG

Welche Unternehmen sind tatsächlich betroffen und haben Handlungsbedarf?

Schritt 1: **rechtliche Abklärung** der Anwendbarkeit

Schritt 2: **technische organisatorische** Umsetzung

Schritt 1: Rechtliche Abklärung

a) Tätigkeit in der EU ausgeübt
b) Unternehmen in einem Sektor der Richtlinie
c) Unternehmensgröße

ACHTUNG:

- verbundenes oder Partner-Unternehmen
- Lieferkette (indirekt über Kunden betroffen)

Schritt 1: Rechtliche Abklärung

<u>Dokumentation</u> der vorgenommenen Abklärung

- **was wurde geprüft (Checkliste)**
- **welche Entscheidungskriterien**
- **Entscheidung ja/nein**

Hinweis

Alle Informationen in diesem Vortrag sind nach bestem Wissen und Gewissen zusammengestellt.

Der Vortragende weist jedoch darauf hin, dass keine Haftung für die Richtigkeit, Aktualität und Vollständigkeit übernommen wird.

Insbesondere ersetzt dieser Vortrag keine rechtliche, organisatorische oder technische Beratung im Einzelfall.

Die Präsentation stellt das Thema auszugsweise dar und bildet nur mit den mündlichen Ausführungen des Referenten eine entsprechende Einheit.

Jede Weitergabe der Unterlagen ohne Zustimmung des Referenten ist unzulässig!

Kontakt

DDSB.AT
DATENSCHUTZ & DIGITALISIERUNG

DDSB.AT Beratung GmbH

Mag. iur. Günther Zikulnig

Office Kärnten und Wien:
+43 1 420005050
office@ddsb.at
www.ddsb.at

Eine Stunde Datenschutz

Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union (NIS-2-Richtlinie)

Mag. Judith Leschanz

26. Juni 2024

Ansprechpartner

- Geschäftsführerin der Secur-Data Betriebsberatungs-GmbH
- Data Protection Officer der A1 Group
- Vorstandsvorsitzende des Vereins österreichischer betrieblicher und behördlicher Datenschutzbeauftragter – Privacyofficers.at
- Mitgründerin des Datenschutzvereins Privacy Ring
- Vortragende an der Universität für Weiterbildung Krems

Ab wann gilt NIS-2?

- Derzeit gilt noch NIS (EU) RL 2016/1148 (nunmehr als NIS-1-RL bezeichnet), die mit 6. Juli 2016 als erster Rechtsakt über Cyber Security in der EU verabschiedet wurde und durch Österreich – verspätet – mit 28. Dezember 2018 unter der Bezeichnung **Netz- und Informationssicherheitsgesetz (NISG)** umgesetzt wurde und durch die mit 17. Juli 2019 verabschiedete **Netz- und Informationssicherheitssicherheitsverordnung (NISV)** konkretisiert wurde.
- Die NIS-2-RL ist am 16. Jänner 2023 in Kraft getreten und von den EU-MS **bis 17. Oktober 2024 umzusetzen**. Sie bedingt eine Novellierung des NISG sowie der NISV.

NIS-1 und NIS-2 im Vergleich

- Waren von NIS-1 ca. 100 österreichische Unternehmen betroffen, sind es bei NIS-2 ca. 5.000 – 7.000!
- NIS-1 betraf 7 Sektoren, NIS-2 18 Sektoren.
- Eine wesentliche Neuerung ist die Unterscheidung zwischen **wesentlichen Unternehmen (essential entities)** oder **Sektoren mit hoher Kritikalität**, die in Anhang I der NIS-2-RL angeführt sind und den **wichtigen Unternehmen (important entities)** oder **sonstige kritische Sektoren** lt. Anhang II.
- Ein weiterer Unterschied ist vor allem im Bereich der staatlichen Aufsicht und der Sanktionsmöglichkeiten zu sehen.
- Auch die Sicherheitsrisken in der Lieferkette sind zu beachten.
- Die RL ist konkreter, so schreibt sie einen risikobasierten Ansatz vor.
- Die Unterscheidung zwischen Betreibern wesentlicher Dienste und Anbietern digitaler Dienste entfällt.

NIS-2 – die 18 Sektoren

Sektoren mit hoher Kritikalität (Anhang I)	Sonstige kritische Sektoren (Anhang II)
Energie	Post- und Kurierdienste
Verkehr	Abfallbewirtschaftung
Bankwesen	Produktion, Herstellung und Handel mit chemischen Stoffen
Finanzmarktinfrastrukturen	Produktion, Verarbeitung und Vertrieb von Lebensmitteln
Gesundheitswesen	Verarbeitendes Gewerbe/Herstellung von Waren
Trinkwasser	Anbieter digitaler Dienste
Abwasser	Forschung (fakultativ)
Digitale Infrastruktur	
Verwaltung von IKT-Diensten (B2B)	
Öffentliche Verwaltung	
Weltraum	

NIS-2 Schwellenwerte

Größenklasse	Mitarbeiter (VZÄ)	Jahresumsatz	Jahresbilanzsumme
Klein (KU)	< 50 und	≤ 10 Mio. EUR oder	≤ 10 Mio. EUR
Mittel (MU)	< 250 und	≤ 50 Mio. EUR oder	≤ 43 Mio. EUR
Groß (GU)	≥ 250	> 50 Mio. EUR und	> 43 Mio. EUR

NIS-2 Ausnahmen und doch keine!

KU fallen nicht unter die NIS-2-RL, **außer** es handelt sich um:

- Vertrauensdiensteanbieter
- Anbieter öffentlicher Kommunikationsnetze oder Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste
- TLD-Namensregister und DNS-Diensteanbieter, ausgenommen Betreiber von Root-Namensservern
- Unternehmen, die alleiniger Anbieter eines Service in einem Mitgliedstaat sind, das essentiell für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Aktivitäten ist

NIS-2 – Risikobasierter Ansatz

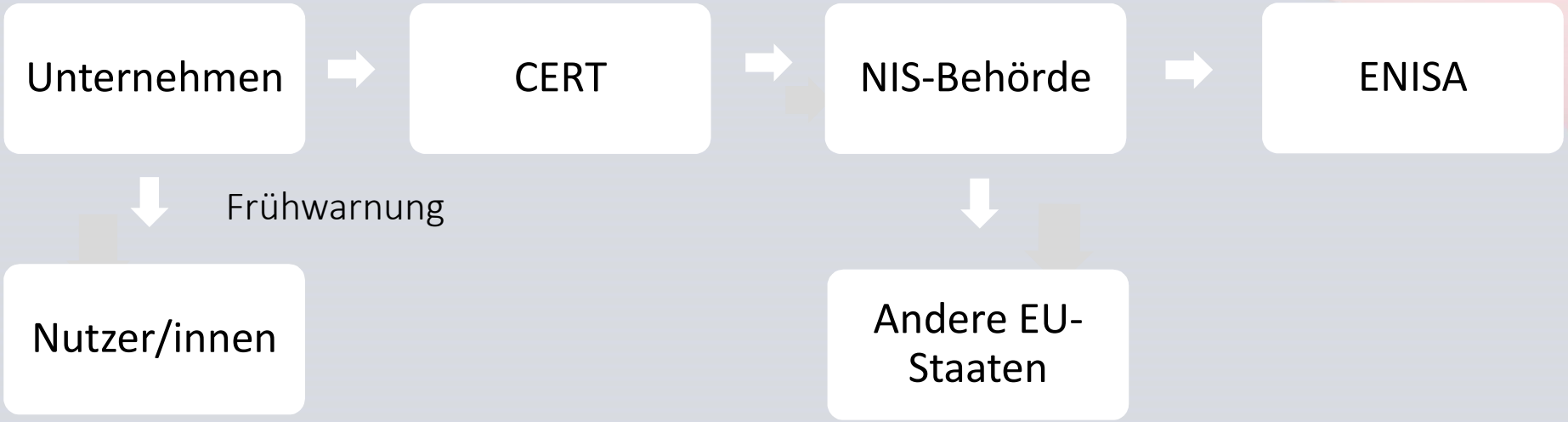
Unter Berücksichtigung folgender Faktoren

- Stand der Technik
- europäischer internationaler Normen
- bestehendes Risiko

(Fortsetzung nächste Seite)

NIS-2 – Berichtspflichten

Meldeweg:



Fristen:

Frühwarnung → unverzüglich bis max. **24 Stunden**

Meldung an die Behörde → unverzüglich bis max. **72 Stunden** nach Kenntnisnahme

Abschlussmeldung → 1 Monat nach Meldung

NIS-2 – Aufsicht und Sanktionen

Was sind die Unterschiede, ob ein Unternehmen als wesentlich oder wichtig gilt?

Ob man als Unternehmen eine wesentliche oder eine wichtige Einrichtung im Sinne der Richtlinie ist, macht bei der Umsetzung der geforderten Sicherheitsmaßnahmen keinen Unterschied.

Es gibt jedoch Unterschiede bei der Aufsicht und den Sanktionen:

Wesentliche Einrichtungen

- regelmäßige und gezielte Sicherheitsprüfungen („ex-ante“)
- Stichprobenkontrollen
- Bußgeldrahmen 10 Mio. Euro oder 2 Prozent des weltweiten Umsatzes (je nachdem, welcher Betrag höher ist)

Wichtige Einrichtungen

- Überprüfungen nur bei begründetem Verdacht („ex-post“)
- Vor-Ort-Kontrollen und externe nachträgliche Aufsichtsmaßnahmen
- Bußgeldrahmen 7 Mio. Euro oder bei 1,4 Prozent des weltweiten Umsatzes

Leitungsorgane (GF, Vorstände) haften bei Verstößen!

Quelle: wko.at

Diskussion

Vielen Dank für Ihre Aufmerksamkeit

Besuchen Sie uns auch im Internet!
Sie finden uns unter https://www.secur-data.at

Meine E-Mail-Adresse lautet:

j.leschanz@secur-data.at

AFM SOLUTIONS

Eine Stunde Datenschutz

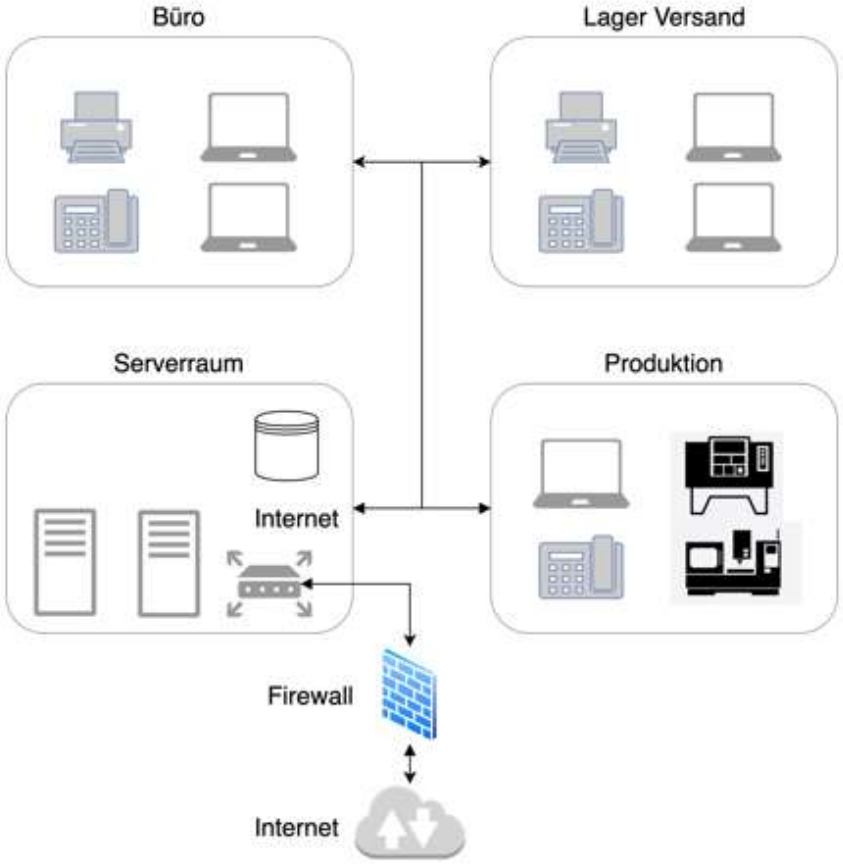
OT Security

Herausforderungen in der OT

- Veraltete Systeme
  - Keine Updates verfügbar
  - Verwendung unsicher Kommunikationsprotokolle (ICS)
- Verwendung von Default-Userberechtigungen bzw. kein Berechtigungssystem vorhanden
- Kein Backup der Konfigurationen und Programme (PLCs)
- Unzureichende Netzwerksegmentierung
- Kein Business Continuity Planning
- Keine Disaster Recovery Procedures
- **Fehlendes Bewusstsein**

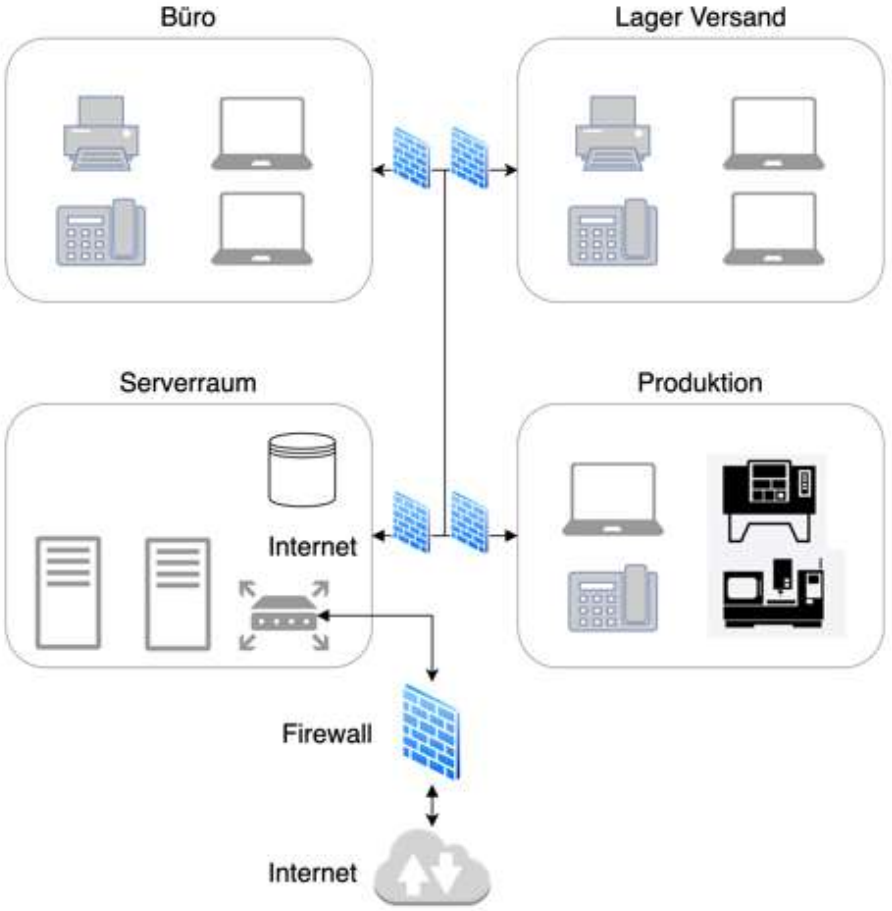
Häufig vorgefunden Ist-Situation im Netzwerk

- Keine Netzwerksegmentierung
- Ungehinderter Internetzugang aus allen Bereichen



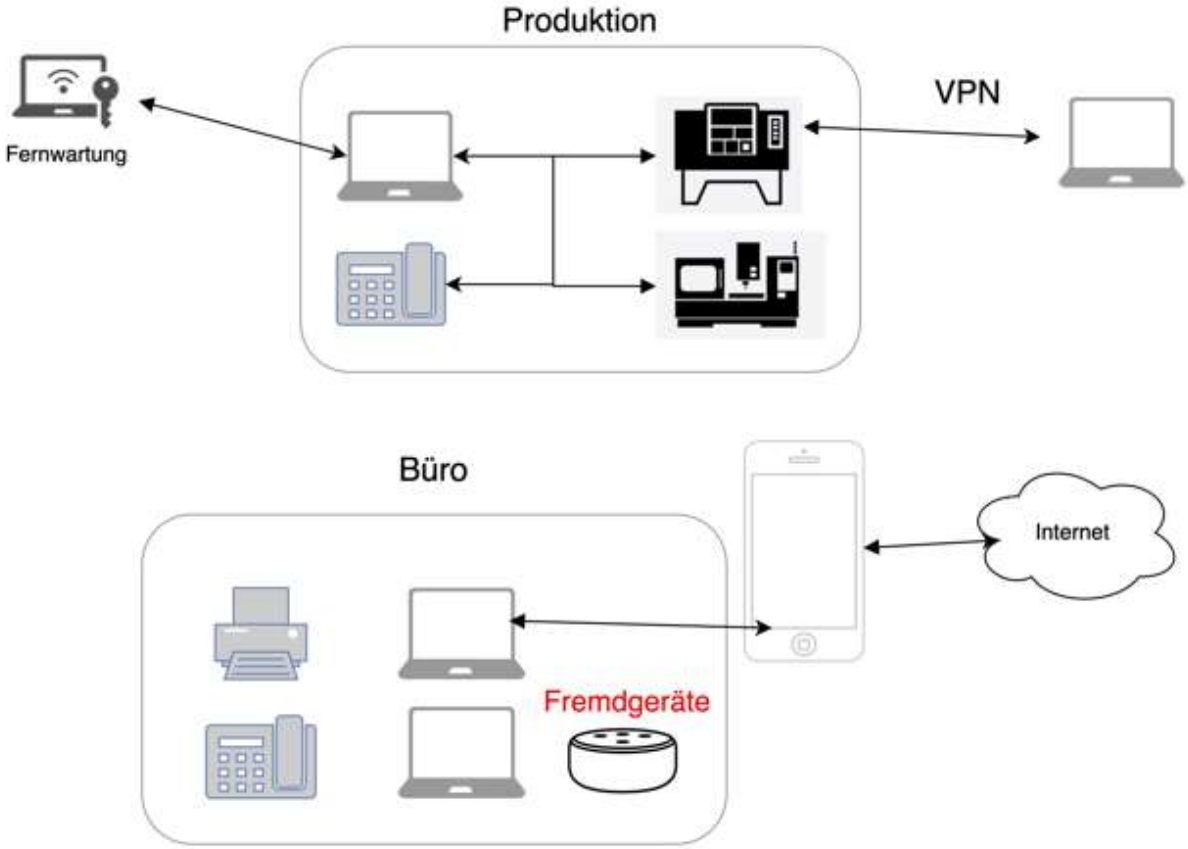
Besser

- Segmentierung nach Funktionsbereichen
- Nutzung von VLANs
- Implementierung nach IEC 62443



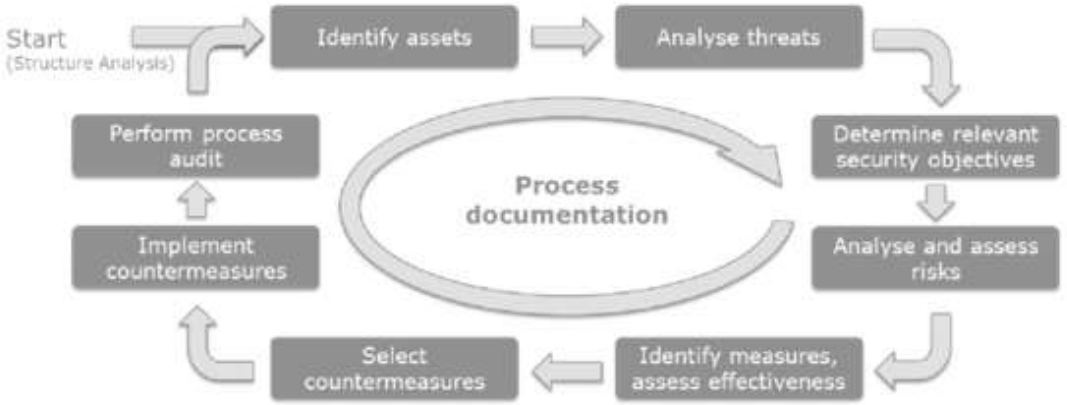
Beachten Sie mögliche Hintertüren

- Unsichere Zugriffe durch Wartungsfirmen oder Hersteller
- Fremdgeräte im Firmennetzwerk
- Unsichere Cloudanwendungen
- Ungewollte Internetzugriffe auf Geräten per Hotspot
- Besucher kommen über das WLAN ungehindert ins Firmennetzwerk bzw. könne sich ins LAN einklinken



Mögliche nächste Schritte

- Erfassung des IST-Zustandes
- GAP-Analyse
- Implementierung
- Unter Beachtung der VDI/VDE 2182 „Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell“



Nutzen Sie NIS2 als Katalysator für die Cyber Security

Vielen Dank für die Aufmerksamkeit!

address Adi-Dassler-Gasse 2, 9073 Klagenfurt / Austria
e-mail office@afm-solutions.at
phone +43 664 1332390

Beratungs- und Fördermöglichkeiten auf dem Weg zu einer adäquaten Cyber-Security

Ing. Walter Wratschko

26. Juni 2024

Beratungsangebot der Wirtschaftskammer Kärnten

- Die NIS2-Beratungen sind für die Unternehmen dank dem Servicezentrum der Wirtschaftskammer Kärnten kostenlos

- Juristische Abklärungen dürfen bis zu 4 Stunden dauern

- Technische und prozessorientierte Beratungen werden jeweils bis zu 3 Stunden vom Servicezentrum finanziert

- Den von den Wirtschaftskammermitgliedern ausgesprochenen Beraterwünsche werden natürlich Folge geleistet, sofern es ein gelisteter Berater ist. Es sollte der Unternehmer die Beratung beim Servicezentrum anfordern, nicht der Berater.

- https://www.wko.at/ktn/wirtschaftsrecht/foerderangebot-nis2

- https://www.wko.at/ktn/information-consulting/unternehmensberatung-buchhaltung-informationstechnologie/das-sind-die-nis2-berater

KMU.digital-Förderungen

1.Statusanalyse IT- und Cybersecurity:

Überprüfung der Sicherheit der digitalen Infrastruktur und Empfehlungen zur Verbesserung; *80% der Nettosumme wird gefördert - max. € 400,-*

2. Strategieberatung von IT- & Cybersecurity:

Analyse von Schwachstellen in der IT-Infrastruktur und Planung der Maßnahmen zur Verbesserung – 50 % Zuschuss - max. 1.000 €

3.Umsetzung im Bereich IT- & Cybersecurity:

Einführung oder Verbesserung der IT- und Cybersecurity-Maßnahmen und -Prozesse oder Aufbau eines Informationssicherheitsmanagements im Unternehmen

4.Umsetzung im Bereich Digitale Verwaltung:

Nutzung der digitalen Verwaltung durch Maßnahmen wie Einführung einer digitalen Signatur oder elektronische Beschaffungsvorgänge

Umsetzungsförderungen: jeweils 30% - max. 6.000 € pro Tool

KWF Digitalisierungs.IMPULS

- Förderung für Kleinst- und Kleinunternehmen
- Dieses Produkt unterstützt Digitalisierungsprojekte innerhalb der drei Schwerpunkte E-Commerce, Geschäftsprozesse und IT-Sicherheit.
- Die Förderung wird in Form eines nicht rückzahlbaren Zuschusses gewährt und beläuft sich auf bis zu 50 % der förderbaren Kosten für Kleinstunternehmen und Kleinunternehmen.
- Die förderbaren Projektkosten müssen mindestens EUR 5.000,- betragen und können bis max. EUR 25.000,- anerkannt werden.
- Die Einreichung ist – je nach budgetärer Verfügbarkeit – von 1. März bis 30. Sept. 2024 möglich.
- (Verlängerung wurde in den letzten Tagen beschlossen)

Arbeitskreis **Datenschutz**

WIRTSCHAFTSKAMMER KÄRNTEN

Ing. Walter Wratschko

Externer Datenschutzbeauftragter
Experte für Brüsseler IT-Richtlinien

Brunnplatz 5, 9020 Klagenfurt
+43 699 15043860

www.datenschutz-sued.at
www.myperfect.it

Terminaviso

Nächste Folge „Eine Stunde Datenschutz“ findet im Herbst statt.

Wir geben den Termin noch bekannt!