CAR Master training

VZDELÁVACIA JEDNOTKA 4

DIGITÁLNE KOMPETENCIE

Co-funded by the European Union

Financované Európskou úniou. Vyjadrené názory a názory sú však len názormi autora (autorov) a nemusia nevyhnutne odrážať názory Európskej únie alebo Európskej výkonnej agentúry pre vzdelávanie a kultúru (EACEA). Európska únia ani agentúra EACEA za ne nemôžu niesť zodpovednosť.

1 Digitálne kompetencie

1.1 Úvod

V profesionálnom aj súkromnom živote sa dnes už len veľmi zriedkavo stretneme s človekom, ktorý vôbec nepoužíva **počítače alebo smartfóny**. Väčšina ľudí teda má určité **základné znalosti o možnostiach a nástrojoch**, ktoré nám počítače a internet poskytujú. Problém však spočíva v skutočnosti, že sa veci neustále menia – niektoré témy naberajú na dôležitosti a iné ustupujú do úzadia. Ako skvelý príklad poslúžia online schôdze, ktoré sa v dôsledku pandémie vírusu COVID-19 stali v mnohých spoločnostiach štandardom.

Definícia

Digitálne kompetencie zahŕňajú „sebavedomé, kritické a zodpovedné využívanie digitálnych technológií pri vzdelávaní, v práci a pri účasti na živote spoločnosti. Digitálna kompetencia ja definovaná ako kombinácia vedomostí, zručností a postojov.“ (Odporúčanie Rady o kľúčových kompetenciách pre celoživotné vzdelávanie, 2018)

Neustále **obnovovanie a rozvíjanie digitálnych zručností** je veľmi užitočné tak v práci, ako aj v súkromnom živote. V tomto školiacom module sa preto budeme venovať štyrom témam zameraným na zlepšenie digitálnych zručností.

Pozrieme sa na **bezpečnostné aspekty v digitálnom priestore** a vysvetlíme, ako sa môžete chrániť pred útokmi hackerov, ako zabezpečiť svoje pracovné a súkromné zariadenia, aby boli neustále chránené, a čo je to počítačová kriminalita.

Okrem toho sa budeme zaoberať **základmi práce s tabuľkami** v programe Microsoft Excel a tým, ako v ňom môžete vyhodnocovať a prezentovať údaje; ukážeme vám, ako správne používať aplikácie **Zoom** a **Microsoft Teams.**; a na záver vám ponúkneme stručný prehľad o tom, ako vytvárať atraktívne prezentácie na počítači, ako aj o **užitočných prezentačných technikách** všeobecne.

Po absolvovaní tohto školiaceho modulu budete:

- Chápať základné charakteristiky bezpečnosti údajov.
- Rozumieť pojmom počítačová kriminalita a hacking.
- Vedieť rozpoznať škodlivé a nevyžiadané e-maily.
- Poznať opatrenia na fyzické zabezpečenie počítačov a mobilných zariadení.
- Ovládať dôležité matematické a štatistické funkcie programu Excel.
- Vedieť primerane vizualizovať údaje.
- Vedieť vytvoriť kontingenčnú tabuľku.
- Poznať filtre a nástroje na analýzu údajov.
- Poznať najdôležitejšie funkcie programov ZOOM a Teams.
- Ovládať najdôležitejšie pravidlá slušného správania v digitálnom priestore.
- Poznať základné prezentačné techniky.
- Vedieť, ako vhodným spôsobom navrhnúť obsah.

1.2 Digitálna bezpečnosť

Pokiaľ ide o budovanie digitálnych zručností, bezpečnosť údajov je v tejto oblasti ústrednou a zastrešujúcou témou. **Údaje a informácie** v našom prepojenom svete predstavujú pre mnohých **hodnotnú menu**. Ale ako každú formu meny, aj údaje možno ukradnúť, čo platí rovnako v súkromnom kontexte, ako aj v profesionálnom. Ak napríklad vyhľadáme v prehliadači Google recept na najlepšiu pečenú fazuľu a prezradíme tým, že sme fanúšikmi anglickej kuchyne, je to jedna vec. Ale ak na falošnej webovej stránke zadáme údaje o svojom bankovom účte, je to niečo úplne iné.

Otázka bezpečnosti údajov sa v súčasnosti stáva čoraz závažnejšou aj v profesionálnom kontexte – **priemyselná špionáž, útoky hackerov a krádeže údajov** sa vyskytujú čoraz častejšie a môžu mať vážne ekonomické dôsledky. A keďže sa najslabšie ohnivko reťaze zvykne pretrhnúť, mal by každý zamestnanec rozumieť aspoň základom bezpečnosti údajov.

Poznámka

Informácie v podstate predstavujú vedomosti alebo podrobnosti o veciach či procesoch.

Údaje sú štandardizované alebo systematické (porovnateľné) informácie určené na ďalšie spracovanie a uchovávanie. Možno ich triediť, vyhodnocovať a používať alebo ukladať v rôznych aplikáciách. V uloženej forme môžete napríklad použiť údaje o adrese na vytvorenie formulára listu; s uloženými číselnými údajmi môžete vykonávať výpočty.

Najprv sa teda pozrime na tri najdôležitejšie prvky bezpečnosti údajov:

- dôvernosť
- integrita
- dostupnosť

Dôvernosť znamená ochranu údajov pred **neoprávneným zverejnením**. Odborné aj súkromné informácie vždy podliehajú určitej úrovni dôvernosti, čo znamená, že sú dostupné len obmedzenej alebo oprávnenej skupine osôb. Dôverné údaje teda môžu prezerať, spracovávať a prenášať len oprávnené osoby.

Príklad

Vyšetrovateľská služba bezpečnostného spravodajstva podniku Gigafactory Berlin-Brandenburg
Vyšetrovateľská služba bezpečnostného spravodajstva je zodpovedná za ochranu duševného vlastníctva, obchodných tajomstiev a dôverných informácií spoločnosti Tesla. Na tejto pozícii budú vyšetrovatelia viesť proaktívne aj reaktívne vyšetrovania a aktívne riešiť interné či externé hrozby pre vlastnícke a dôverné informácie spoločnosti Tesla. Budú podliehať manažérovi pre vyšetrovanie v regióne EMEA.

Integrita znamená v tomto kontexte schopnosť zabezpečiť, že **údaje ostanú nezmenené a úplné** a že všetky príslušné systémy budú fungovať správne. Pokiaľ teda chceme zaručiť integritu údajov, nemôžu sa dať nepozorovane zmeniť a nemôže sa s nimi dať manipulovať – všetky vykonané zmeny sa musia dať odsledovať a spätne vyhľadať.

Dostupnosť znamená, že údaje, siete, softvér aj hardvér sú k dispozícii vždy, **keď ich treba** – napríklad počas úradných hodín. Potrebné údaje preto nesmú vedieť zablokovať neoprávnené osoby.

Poznámka

Dôležité sú aj ďalšie dva pojmy: **Autentickosť** dokazuje, že osoba, ktorá údaje odosiela alebo prenáša, je tou osobou, za ktorú sa vydáva. Autentickosť osoby sa preto musí dať overiť.

Záväznosť sa týka „nepopierateľnosti" zmien údajov. To znamená, že údaje sú záväzné, ak ich vytvorenie alebo zmenu možno jasne a nepochybne priradiť určitej osobe.

Zabezpečením uvedených znakov sa snažíme zabezpečiť údaje. Útoky na tieto prvky alebo pokusy o ich obchádzanie v podstate spadajú pod počítačovú kriminalitu, ktorú nazývame aj **kyberkriminalita**.

Počítačová kriminalita je v zmysle Trestného zákona trestný čin a zahŕňa všetky **trestné činy** spáchané **pomocou informačných alebo komunikačných technológií alebo proti nim**. Patrí sem napr.:

- počítačový podvod, t. j. akákoľvek forma podvodu spáchaná prostredníctvom počítača alebo internetu,
- sledovanie alebo zachytávanie údajov a ich ďalší predaj,
- falšovanie údajov alebo sabotáž počítačových systémov,
- porušovanie autorských práv a ochranných známok.

Príklad

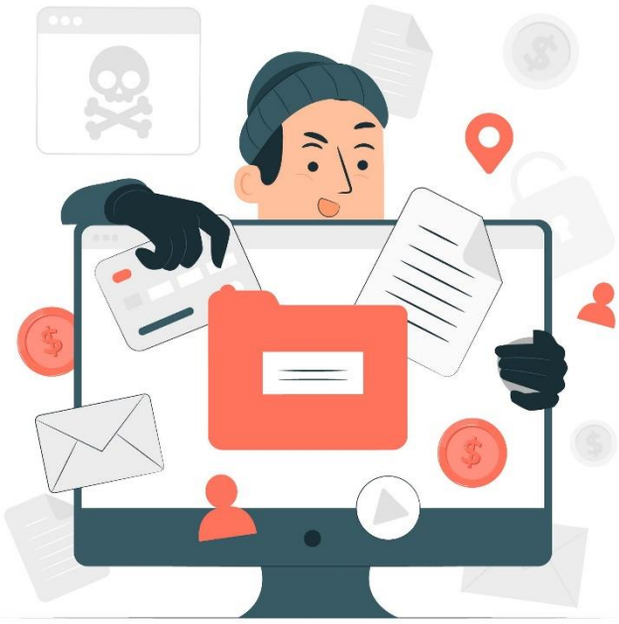
Automobilový priemysel sa považuje za najväčšie priemyselné odvetvie v Nemecku, ktoré generuje tržby vo výške viac ako 411 miliárd eur. Nemecko je tak z hľadiska výroby automobilov najväčšou krajinou v Európe, o čom svedčí aj fakt, že sa tu v roku 2021 vyrobilo až 30 % všetkých osobných automobilov vyrobených v EÚ. Odvrátenou stranou tejto mince však je, že sa automobilové spoločnosti, ich zamestnanci a používatelia ich produktov často stávajú terčom rôznych útokov kyberzločincov. Ako nedávny príklad poslúži kampaň na krádež informácií, ktorá sa zamerala na zákazníkov nemeckých spoločností, najmä predajcov automobilov, prostredníctvom phishingových e-mailov, ktorých cieľom bolo infikovať obete malvérom na krádež informácií.

Ďalší nedávny kybernetický útok, ku ktorému došlo v marci 2022, sa zameral na nemeckú dcérsku spoločnosť japonského dodávateľa automobilov Denso. Ransomvérová skupina Pandora oznámila, že infiltrovala sieť, a na svojom blogu zdieľala snímky obrazoviek objednávok, technických schém automobilov a e-mailov. Okrem toho jej členovia tvrdili, že zo spoločnosti ukradli 1,4 TB údajov. Po útoku sa spoločnosť Denso ospravedlnila za spôsobené nepríjemnosti a potvrdila, že do nemeckej siete niekto získal nezákonný prístup.

Vzhľadom na to, že čoraz viac vozidiel je pripojených na internet a využíva množstvo digitálnych funkcií, veľké automobilové spoločnosti vystavujú autá ďalším škodlivým aktivitám a zvyšujú riziko kybernetických útokov.
Zdroj: https://ke-la.com/resource/german-automotive-sector-cybercrime-threats-landscape-report/

V súvislosti s počítačovou kriminalitou sa nám prirodzene vybaví pojem „**hacking**“. Toto slovo pôvodne znamenalo jednoducho identifikáciu kreatívneho postupu riešenia technického problému. V bežnej reči sa však hacking ustálil skôr v negatívnom zmysle. Označuje totiž prípady, v ktorých niekto získa **nezákonný a neoprávnený prístup do počítačových systémov alebo sietí**.

Hacking spadá pod počítačovú kriminalitu a je teda trestným činom. Môže postihnúť súkromné osoby, ktorým z počítačov ukradli údaje o kreditných kartách alebo iné osobné informácie, no postihuje aj celé spoločnosti či dokonca vlády. **Priemyselná špionáž** je napokon bežná najmä vo vysoko konkurenčných odvetviach.



https://www.freepik.com/free-vector/data-stealing-malware-concept-illustration_18771508.htm#query=cyber%20crime&position=47&from_view=search&track=sph

Bežný útok hackerov prebieha prostredníctvom tzv. phishingových e-mailov. Posielajú sa falošné e-maily, ktoré prekabátia prijímajúcu osobu a vyzvú ju, aby zadala osobné alebo pracovné údaje (prístupové údaje, heslá atď.) či dokonca klikla na odkazy, ktoré potom stiahnu neželaný softvér (často nepozorovane).

Príklad

1. Podvod s falošnou faktúrou

Začnime pravdepodobne najpopulárnejšou šablónou phishingu – technikou falošnej faktúry. Podobne ako mnohé iné phishingové útoky, aj tento podvod sa spolieha na strach a naliehavosť, pričom na koncového používateľa vyvíja nátlak, aby odoslal platbu za tovar či služby, ktoré si však nikdy neobjednal ani nedostal.

2. Podvod s aktualizáciou e-mailového účtu

Pri podvode, ktorý sa týka aktualizácie e-mailového účtu, čelíte pomyselnej hrozbe, že vášmu kontu vyprší platnosť, ak okamžite nepodniknete určité kroky. Môže sa zdať, že e-mail pochádza od dôveryhodných poskytovateľov e-mailových služieb, ako sú Microsoft a Google, alebo jednoducho od IT oddelenia vašej spoločnosti. Užitočná rada – pri výzve na zadanie osobných údajov prejdite myšou ponad odkaz, keďže samotný text často nepredstavuje skutočný cieľ odkazu.

3. Podvod so službou PayPal

Tieto e-maily často obsahujú logo služby PayPal a navyše presvedčivé drobné písmo v spodnej časti e-mailu. Tento podvod sa opäť snaží vyvolať v obetiach paniku, často správou typu: „Vo vašom účte sa vyskytol problém, kliknite sem a vyriešte ho“. Pozor, tieto správy obsahujú aj legitímne vyzerajúce drobné písmo.

Podobné podvodné e-maily je niekedy dosť ťažké identifikovať. Nasledujúce tipy vám však väčšinou pomôžu rozlíšiť ich:

- neprimeraný počet pravopisných a gramatických chýb,
- použitie cudzieho jazyka,
- neosobný pozdrav, napríklad „Vážený používateľ“ (pozor, niekedy môžu hackeri pri phishingu zistiť aj skutočné mená a osobný pozdrav preto nie je zárukou správnosti e-mailu),
- výzva na vykonanie nejakej akcie, prípadne aj pod hrozbou (napr.: „Zadajte čo najskôr údaje o svojom účte, inak sa vám zablokuje účet.“),
- všeobecné žiadosti o zadanie údajov, otvorenie súboru alebo otvorenie akýchkoľvek odkazov.

Poznámka

Ak si myslíte, že ste dostali falošný e-mail, okamžite to nahláste svojej spoločnosti. V žiadnom prípade naň neodpovedajte, nevolajte na žiadne telefónne čísla a neklikajte na odkaz ani len „na skúšku“.

Samozrejme, údaje sa dajú ukradnúť aj inak ako cez internet, a preto ich treba zabezpečiť aj fyzicky. K strate údajov môže dôjsť aj pri zničení hardvéru, infikovaní vírusom, vymazaní údajov omylom alebo úmyselne, alebo jednoducho krádežou zariadenia. Existujú preto rôzne opatrenia na fyzické zabezpečenie zariadení, ako sú notebooky, firemné a súkromné mobilné telefóny a tablety:

- Miestnosti s hardvérom bez dozoru vždy zamknite.
- Nespúšťajte (najmä prenosné) zariadenia z dohľadu.
- Zabezpečte prístup do miestností s hardvérom pomocou systémov magnetických kariet alebo hesiel.
- Zariadenia pripútajte bezpečnostnými káblami.
- Nastavte zvukové výstrahy, napríklad ak sa miestny hardvér presunie z obvyklého miesta alebo ak sa osoba, ktorá ho používa, príliš vzdiali od zariadenia.
- Pripevnite k zariadeniam takzvané mikrobodky M-DotDNA (malé bodky lepidla obsahujúce jednotlivé kódy), ktoré používa polícia na identifikáciu zadržaného odcudzeného majetku.

Dôležité

Ďalšiu ochranu predstavuje nastavenie možností diaľkového uzamknutia alebo vymazania. To znamená, že v prípade krádeže možno príslušné zariadenie uzamknúť alebo vymazať údaje na ňom z iného zariadenia.

1.3 Základy programu Microsoft Excel

Teraz, keď už vieme zabezpečiť svoje údaje, sa pozrime na to, čo s nimi môžeme robiť. Údaje môžeme napríklad **usporiadať do tabuliek, následne ich navzájom matematicky či štatisticky prepojiť a napokon prezentovať v grafoch**, aby sme zistili, čo potrebujeme vedieť. Na tento účel sa využíva známy (tzv. „tabuľkový“) program **Microsoft Excel**.

Poznámka

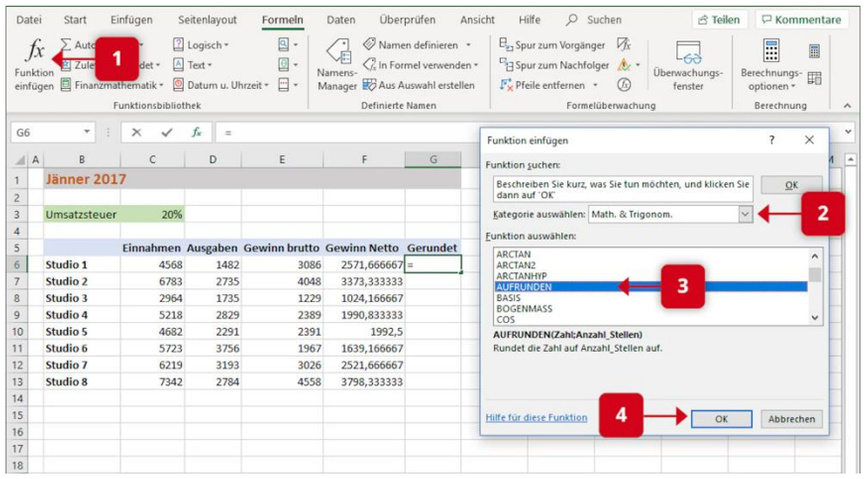
Excel je **tabuľkový program**, ktorý nám poskytuje rozsiahly výber najrôznejších **matematických a štatistických funkcií** na spracovanie údajov. Tieto funkcie predstavujú **preddefinované vzorce argumentov funkcií**, pomocou ktorých sa vykonávajú výpočty. Sú zostavené podľa základnej štruktúry, ktorá je vždy rovnaká („syntax“), a začínajú znamienkom rovnosti (=), za ktorým nasleduje názov funkcie a argumenty funkcie oddelené bodkočiarkou (;).

Pozrime sa na **niekoľko dôležitých matematických funkcií**, ako príklad:

Funkcia:	Popis
ROUND	Zaokrúhľuje číslo na určitú číslicu (5 a viac sa zaokrúhľuje nahor a menej ako 5 sa zaokrúhľuje nadol) – napríklad z 1,44 sa stane 1,4 a z 1,7 sa stane 2,0.
ROUNDDOWN	Zaokrúhľuje číslo nadol na určitý počet desatinných miest smerom k nule.
ROUNDUP	Zaokrúhľuje číslo nahor na určitý počet desatinných miest.
SUM	Vypočíta súčet vybraných buniek.

V praxi to funguje napríklad takto: Číslo v bunke F6 (t. j. stĺpec F, riadok 6) chceme v bunke G6 zobraziť zaokrúhlené na dve desatinné miesta. Najprv teda vyberieme bunku G6 v mriežke a potom vykonáme nasledujúce kroky.

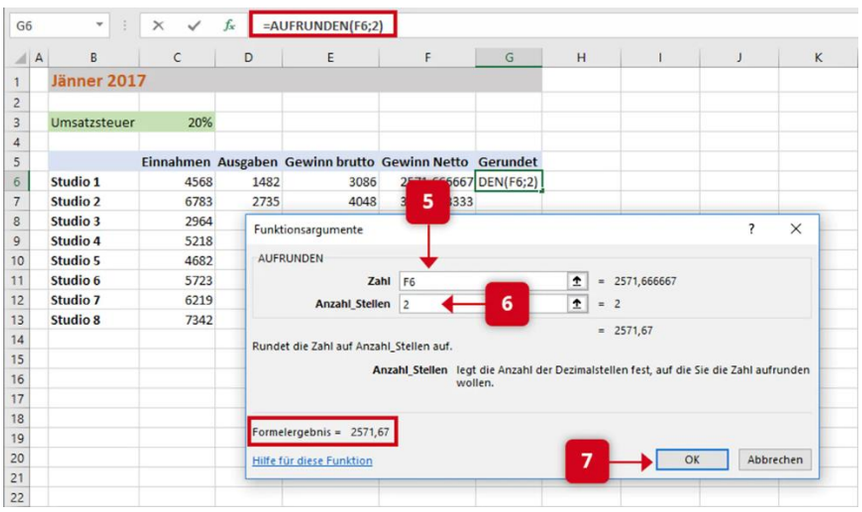
1. Na karte *Vzorce* klikneme na položku *Vložiť funkciu*.
2. V okne, ktoré sa zobrazí, teraz vyberieme kategóriu *Matematické*.
3. V zozname *Vybrať funkciu* vyberieme našu požadovanú funkciu ROUNDUP.



Obrázok 2

Zdroj: bit.academy https://portal.bitacademy.at/module/368/phase/6369/

4. Potom klikneme na tlačidlo *OK* a zobrazí sa dialógové okno *Argumenty funkcie*.
5. Teraz vyberieme naše číslo v bunke F6 ako argument funkcie – buď kliknutím myšou, alebo jednoducho tak, že *F6* napíšeme.
6. Do položky *Počet_číslic* zadáme 2.
7. Stlačením tlačidla *OK* potvrdíme našu funkciu.



Obrázok 3

Zdroj: bit.academy https://portal.bitacademy.at/module/368/phase/6369/

Poznámka

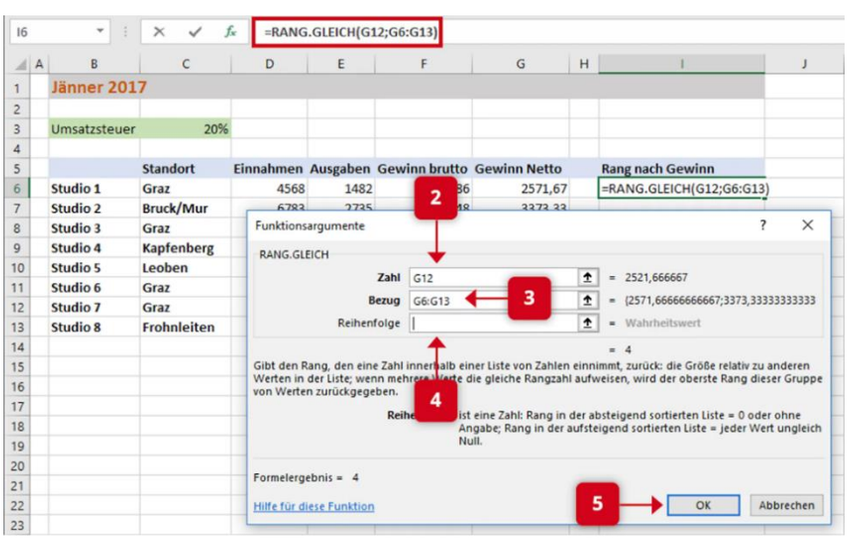
Teraz poznáte základný postup **väčšiny matematických funkcií v programe Excel** – samozrejme, **možnosti v dialógových oknách** sa menia v závislosti od vybranej funkcie. Tip: Pri funkciách, ktoré môžu ovplyvniť celý rozsah čísel, napríklad SUM, môžete príslušný rozsah rýchlo vybrať podržaním tlačidla myši.

Excel nám ponúka aj množstvo **funkcií na štatistické výpočty**. Tu sú najdôležitejšie príklady:

Funkcia:	Popis
COUNT	Určuje počet buniek v určitom rozsahu buniek, ktoré obsahujú hodnoty.
COUNTIFS	Určuje počet buniek v určitom rozsahu buniek, ktoré obsahujú hodnoty a spĺňajú určité kritérium (napríklad obsahujú určitú hodnotu).
RANK.EQ	Pomocou tejto funkcie možno určiť postavenie čísla vybranej bunky v porovnaní s číslami všetkých buniek.
COUNTBLANK	Určuje počet prázdnych buniek v rámci rozsahu buniek.

Štatistická funkcia v programe Excel funguje podobne ako matematická funkcia:

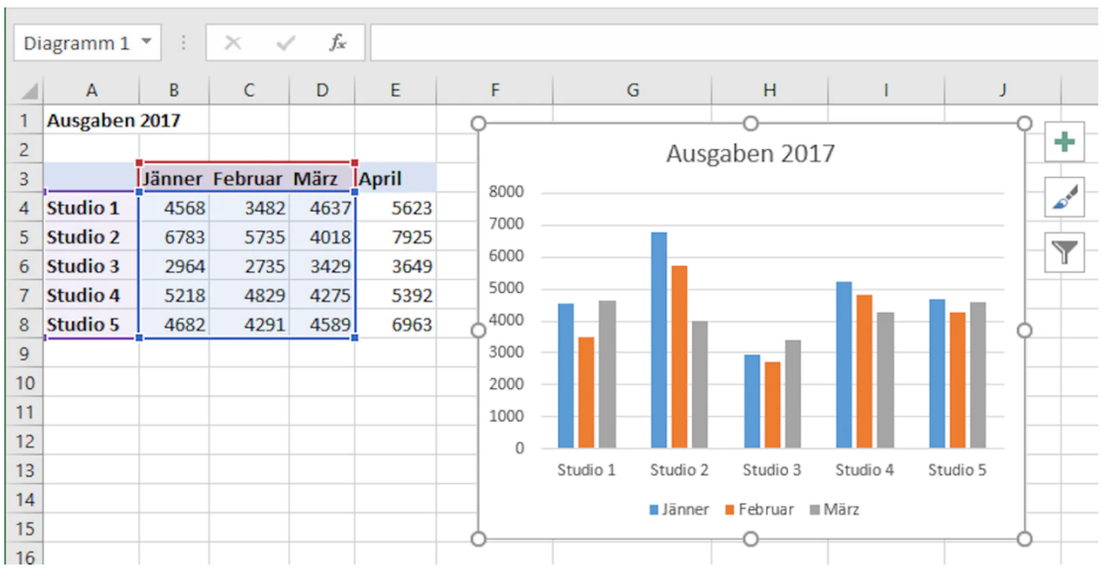
1. V dialógovom okne *Vložiť funkciu* vyberieme kategóriu *Štatistické* a funkciu RANK.EQ.
2. Do poľa *Číslo* napíšeme príslušnú bunku (v našom príklade G12).
3. V poli *Odkaz* vyberieme oblasť nášho rebríčka.
4. V poli *Poradie* určíme, či prvé miesto v poradí obsadí najnižšie (zapíšeme ľubovoľnú hodnotu) alebo najvyššie číslo (pole necháme prázdne).
5. Tlačidlom *OK* potvrdíme funkciu.



Obrázok 4
Zdroj: https://portal.bitacademy.at/module/368/phase/6370/

Excel sa výborne hodí aj na **grafické zobrazenie tabuliek** – môžete napríklad hneď zobraziť rôzne súbory údajov.

K dispozícii sú **stĺpcové, kruhové, koláčové, pruhové a mnohé ďalšie typy** dvoj- alebo trojrozmerných grafov. Príklad na obrázku 5 predstavuje stĺpcový graf.



Obrázok 5
Zdroj: https://portal.bitacademy.at/module/368/phase/6392/

Vytvorenie grafu v programe Excel:

1. Najprv vyberieme všetky hodnoty v tabuľke, ktoré chceme zahrnúť do grafu.
2. Na karte *Vložiť* potom vyberieme položku *Grafy* a požadovaný typ grafu.
3. Graf sa teraz vytvorí automaticky. Údaje môžeme kedykoľvek pridať alebo odstrániť zmenou vybraného rozsahu buniek, ale môžeme tiež upraviť požadovaný dizajn alebo formu zobrazenia kliknutím na symbol plus či štetec.

Dôležité

Jedným z najvýkonnejších nástrojov programu Excel je možnosť vytvárať **kontingenčné tabuľky** a pracovať s nimi. Kontingenčné tabuľky možno použiť aj na štruktúrovanie, analýzu a vyhodnocovanie veľmi veľkých objemov údajov.
Na tento účel sa používajú **rôzne filtre a nástroje na analýzu údajov** – napríklad na to, aby sa inak príliš veľké množstvo údajov zhrnulo či zredukovalo len na tie údaje, ktoré sú potrebné.

Pozrime sa na **príklad použitia kontingenčnej tabuľky**. Máme malú kaviarenskú spoločnosť a chceme analyzovať predaj kávy. Na tento účel máme ako základ nasledujúcu tabuľku:

Nr	Monat	Hersteller	Produkt	Preis	Verkäufer	Kunde
1	Jänner	Lavazza	Lungo	€ 565	Wolf	Gastro Konzept
2	Jänner	Lavazza	Decaffeinato	€ 941	Wolf	Gastro Konzept
3	Jänner	Lavazza	Lungo	€ 764	Kofler	Zweig GmbH
4	Jänner	Segafredo	Espresso	€ 871	Kofler	Zweig GmbH
5	Jänner	Lavazza	Decaffeinato	€ 981	Kofler	Maier Kaffee
6	Jänner	Lavazza	Lungo	€ 682	Kofler	Maier Kaffee
7	Jänner	Segafredo	Lungo	€ 141	Kofler	De Cafe
8	Jänner	Lavazza	Lungo	€ 634	Kofler	Maier Kaffee
9	Jänner	Lavazza	Espresso	€ 1.686	Wolf	Horner KG
10	Jänner	Segafredo	Espresso	€ 561	Wolf	De Cafe
11	Jänner	Segafredo	Lungo	€ 581	Kofler	Horner KG
12	Jänner	Segafredo	Lungo	€ 933	Kofler	Horner KG
13	Jänner	Lavazza	Decaffeinato	€ 634	Wolf	Horner KG
14	Jänner	Lavazza	Lungo	€ 771	Wolf	Horner KG

Kaffeverkäufe

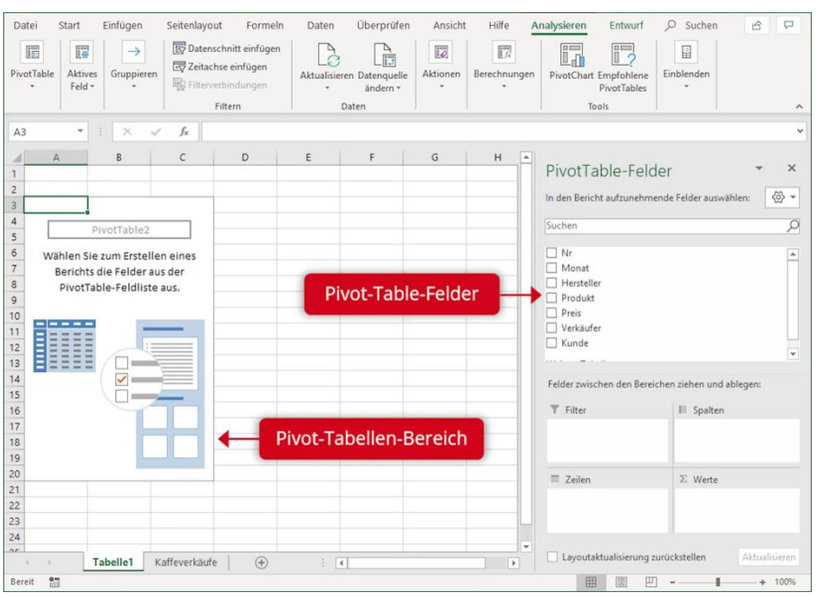
Obrázok 6

Zdroj: https://portal.bitacademy.at/module/368/phase/6413/

Teraz chceme **pomocou kontingenčnej tabuľky** zistiť, **koľko kávy Lavazza sme predali v porovnaní s ostatnými výrobcami**, aké boli **tržby** vo **februári** a aké boli **celkové tržby** v **prvom štvrťroku**.

1. To urobíme tak, že najprv klikneme na ľubovoľnú bunku v tabuľke a potom na nápis *Kontingenčná tabuľka* na karte *Vložiť*. Teraz sa zobrazí príslušné dialógové okno.
2. V ňom sa zvyčajne automaticky rozpozná rozsah buniek našej tabuľky – môžeme to skontrolovať pomocou farebného ohraničenia.
3. Teraz máme možnosť vložiť kontingenčnú tabuľku do nového alebo do existujúceho hárka. Výber potvrdíme tlačidlom *OK*. Teraz sa otvorí nová oblasť úloh.

Obrázok 7

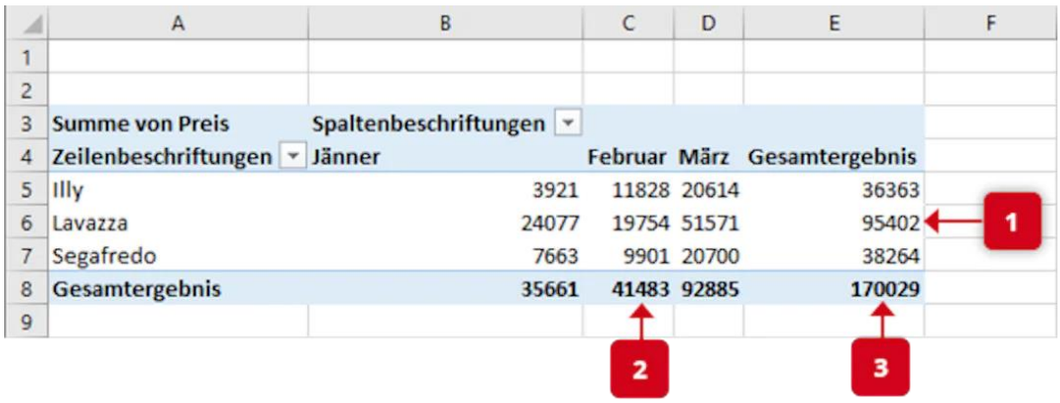


Zdroj: https://portal.bitacademy.at/module/368/phase/6413/

4. Pomocou funkcie ťahaj a pusti môžeme teraz ťahať zo zoznamu rozpoznaných polí (napr. výrobca) do oblastí Filter, Stĺpce, Riadky alebo Hodnoty.

5. Pre naše účely by sa **výrobné spoločnosti** mali zobraziť ako riadky (aby sa dali porovnať príslušné obraty). **Mesiace** sa zobrazujú ako stĺpce. Údaje o obrate vyplývajú z poľa Cena – to pretiahneme do oblasti Hodnoty. Tam sa štandardne nachádza súčet (SUM) hodnôt, ale v prípade potreby ho možno zmeniť.

Obrázok 8



	A	B	C	D	E	F
1						
2						
3	**Summe von Preis**	**Spaltenbeschriftungen**				
4	**Zeilenbeschriftungen**	**Jänner**	**Februar**	**März**	**Gesamtergebnis**	
5	Illy	3921	11828	20614	36363	
6	Lavazza	24077	19754	51571	95402	
7	Segafredo	7663	9901	20700	38264	
8	**Gesamtergebnis**	**35661**	**41483**	**92885**	**170029**	
9						

Zdroj: https://portal.bitacademy.at/module/368/phase/6413/

Výsledkom je kontingenčná tabuľka ako na Obrázku 8. Vidíme **tržby, ktoré dosiahneme z kávy Lavazza v porovnaní s ostatnými výrobcami** (1), **celkové tržby vo februári** (2) a všetky **celkové tržby v prvom štvrťroku** (3).

Dôležité

Kontingenčná tabuľka môže automaticky a správne zachytiť údaje zdrojovej tabuľky len vtedy, ak **nemá prázdne riadky alebo stĺpce**.

1.4 Digitálne nástroje

Mnohé odborné stretnutia sa v súčasnosti konajú v digitálnom priestore – samozrejme, hovoríme o **online stretnutiach** alebo online konferenciách. Existujú rôzne softvéry, ktoré sa používajú v odbornom kontexte. Pre lepšie pochopenie sa pozrime na dva dôležité – **Zoom** a **Microsoft Teams**.

V princípe sú si, samozrejme, podobné. V oboch prípadoch ide o programy, pomocou ktorých môžete **komunikovať online v skupinách alebo dvojiciach prostredníctvom obrazu a zvuku**. Potrebujete účet a e-mailovú adresu a môžete sami vytvárať stretnutia alebo sa na nich zúčastňovať. Počas stretnutia môžete využívať rôzne funkcie. Môžete **zdieľať obrazovku** alebo určité **dokumenty**, no tiež využívať **čety**, v ktorých možno zdieľať odkazy alebo iné správy, či **nástroje, ako sú tabule**, na ktorých môžete spoločne pracovať.

https://www.freepik.com/free-vector/telecommuting-

concept_7938248.htm#query=online%20meeting&position=3&from_view=search&track=sph

Microsoft Teams tvorí súčasť balíka Office 356 a patrí do sveta spoločnosti Microsoft. Je preto dobre integrovaný s ostatnými produktmi tejto spoločnosti. Na druhej strane Zoom je samostatná cloudová videokonferenčná platforma. Obe sú k dispozícii v obmedzených bezplatných verziách a v rôznych platených verziách, ktoré majú rozličné funkcie.

Tip

WBL_GOES_VIRTUAL poskytuje súbor 25 digitálnych nástrojov, ktoré sú vhodné na virtualizáciu procesov vzdelávania na pracovisku. Nástroje pokrývajú rôzne oblasti procesov WBL (vzdelávania založeného na práci), medzi ktoré patrí riadenie vzdelávania, tvorba výučbových materiálov, virtuálna komunikácia a ďalšie procesy. https://www.wbl-goes-virtual.eu/toolbox/

Vo všeobecnosti sa dá povedať, že Microsoft Teams využívajú skôr veľké spoločnosti. Je to najmä preto, že sa používa ako súčasť celého softvérového balíka – teda ak potrebujete viac ako len videokonferencie v pracovnom prostredí. Na druhej strane je Zoom prístupnejší pre menšie skupiny ľudí (najmä ak ide len o videokonferencie), aj keď je potrebné zapojiť napríklad účastníkov mimo firmy.

Pozrime sa teda na porovnanie jednotlivých výhod a nevýhod:

	Microsoft Teams	Zoom
Výhody	Súčasť komplexného softvérového balíka Microsoft. Ochrana údajov na vysokej úrovni. Časový limit pre stretnutia v bezplatnej verzii: 60 minút. Platené verzie sú o niečo lacnejšie.	Veľmi jednoducho sa používa. Viac ako 1 000 ďalších funkcií a integrácie so softvérom tretích strán. Veľmi dobrá kvalita zvuku a videa.
Nevýhody	Platené verzie sa platia na rok. Integrácia so softvérom, ktorý nie je od spoločnosti Microsoft, je značne obmedzená.	Platené verzie sú drahšie. Časový limit pre stretnutia v bezplatnej verzii: 40 minút. V minulosti sa vyskytli problémy s ochranou údajov.

Mimochodom: Rovnako ako na analógovom pracovisku, napríklad v kancelárii, aj v digitálnom priestore by ste mali dodržiavať určité normy slušného správania. Tu uvádzame niekoľko dôležitých vecí, na ktoré treba pamätať:

- Pri práci z domu by **nemalo byť príliš vidieť súkromnú sféru** – čo najneutrálnejšie pozadie bez akýchkoľvek záblesko v súkromného životného prostredia zaručuje profesionalitu a neruší počas rozhovoru. To, že by ste ~~že~~ počas rokovania mali ostať v obraze a vyhýbať sa vareniu či robeniu akýchkoľvek súkromných vecí bokom, je pritom samozrejmosť.
- Bezchybné **pripojenie na internet**, kvalitné **slúchadlá a mikrofón** a vhodná **webkamera** zabezpečia, že budete dobre rozumieť kolegom a aj oni vám. Každé stretnutie trpí nekvalitným obrazom alebo zvukom.
- **Nemali by ste miešať osobné a pracovné** sociálne siete (napríklad LinkedIn alebo Facebook). Vyhnite sa žiadostiam o kontakt od manažérov alebo klientov a na sociálnych sieťach nezverejňujte profesionálne alebo dôverné údaje.
- Pri preposielaní e-mailov dbajte na to, aby ste z nich **odstránili zbytočné predchádzajúce e-maily** – pre prijímajúcu osobu je to prehľadnejšie.
- Tiež si naplánujte **online schôdzky len počas bežných pracovných hodín**, napríklad medzi 9. a 17. hodinou (a nie počas obeda).

Poznámka

Ak sa budete správať ako v kancelárii, v zásade nemôžete nič pokaziť. Nezabúdajte, že **digitálny priestor je tiež verejný**, a teda zdvorilosť a profesionalita sú rovnako dôležité ako v bežnom pracovnom prostredí.

Povedzme, že ste pripravili a analyzovali údaje pomocou kontingenčnej tabuľky – teraz, samozrejme, chcete (alebo potrebujete) výsledky zaujímavým spôsobom **prezentovať**. Preto sa na záver pozrieme na niektoré základy digitálnych prezentačných techník.

Pri prezentácii sú dôležité dva aspekty: na jednej strane technické nástroje, ktoré používate, a na druhej strane vaše vystupovanie (t. j. hlas, reč tela a vonkajší vzhľad) a to, čo hovoríte po obsahovej stránke.

Keď sa povie technické nástroje, prirodzene si ako najznámejší prezentačný softvér ihneď vybavíme **Microsoft PowerPoint**. Existuje však aj iné softvéry, ktoré vám môžu poslúžiť a na ktoré by ste nemali zabúdať:

- **Prezentačný softvér:** Okrem PowerPointu existujú napríklad aj **Pages** (od spoločnosti Apple) a **Google Slides** (obzvlášť dôležitý, ak spoločnosť interne pracuje so službami Google), ale aj bezplatné softvéry, ako sú LibreOffice a Apache OpenOffice.
- **Interaktívny softvér:** Pomocou programov, ako je **Miro**, môžete prostredníctvom digitálnych tabúľ priblížiť obsah svojmu publiku „naživo“. Nástroje na spoluprácu, ako sú **Google Docs** alebo **Slido**, môžete použiť na zapojenie publika do aktivít, ako je brainstorming alebo hlasovanie.

Dôležité

Pri online prezentáciách zvyčajne „zdieľate“ svoju obrazovku so všetkými účastníkmi – to znamená, že to, čo vidíte na svojej obrazovke, vidia aj všetci ostatní. Vďaka tomu **je veľmi jednoduché používať prezentačný a interaktívny softvér** – niekedy je dokonca už integrovaný (napríklad funkcia bielej tabule). Dbajte však na to, aby ste **mali otvorený len obsah, ktorý patrí do prezentácie**.

Pri samotnej prezentácii sú veľmi dôležité dva faktory: **jej atraktívny dizajn** a **váš sebavedomý a sebaistý vzhľad**. Vaše publikum chce predsa dostať spoľahlivé a zrozumiteľné informácie. Na dosiahnutie profesionálneho vzhľadu vám pomôžu nasledujúce tipy:

- **Reč tela:** Vždy sa otočte smerom k publiku a dbajte na to, aby ste udržiavali vhodný očný kontakt so všetkými zúčastnenými. Používajte ruky a zaujmite vzpriamený postoj. Vyhnite sa spínaniu rúk alebo ich vkladaniu do vreciek nohavíc.
- **Hlas:** Vždy hovorte zreteľne a príjemným tempom. To platí najmä pre prezentácie, ktoré sa uskutočňujú v rámci online stretnutia. Dobrá intonácia pri najdôležitejších častiach vašej prezentácie ju pomôže oživiť.
- **Príprava a vzhľad:** Vždy sa pripravte na prezentáciu a na všetky otázky, ktoré sa môžu vyskytnúť – prezentáciu tak dokážete zrozumiteľne predniesť aj v prípade nepredvídaných problémov (napríklad ak váš prezentačný nástroj nefunguje). Dbajte na to, aby ste boli vhodne oblečení (radšej príliš elegantne ako príliš ležérne) a upravení – a to aj v prípade, že prezentáciu prednášate z domu.
- **Reagujte na publikum:** Ak si všimnete, že vaše publikum niečomu nerozumie, opýtajte sa ho a zapojte ho do prezentácie. Pomôže vám to udržať si pozornosť poslucháčov. Pri dlhých prezentáciách môžete v prípade potreby zaradiť aj malé prestávky.

Poznámka

Váš vzhľad rozhoduje o pôsobivosti prezentácie. Prezentačný softvér je len nástroj na názornejšie sprostredkovanie obsahu. Aj tu by ste však mali mať na pamäti pár vecí:

Dbajte na jednotný dizajn a rozloženie prezentácie, nech nie je neprehľadná. Dodržiavajte **pravidlo KISS** (z anglického Keep It Straight And Simple – nech je to priame a jednoduché) – jednotlivé snímky musia byť **jednoduché**, **prehľadné** a **krátke**. Vyhnite sa nadbytočnosti a svoju prezentáciu vnímajte skôr ako nadstavbu – **zodpovedajúce obrázky alebo grafy** môžu v kombinácii s tým, čo hovoríte, urobiť veľký dojem. Ak v prezentácii používate text, uistite sa, aby bol primerane veľký, najmä ak sa prezentácie zdieľajú na obrazovkách počítačov na online schôdzkach.

1.5 Zhrnutie

Čo sme sa naučili

V našom presieťovanom svete predstavujú **údaje** a **informácie** pre mnohých **cenné platidlo**. Ľudia a spoločnosti chcú ochranu pred priemyselnou špionážou, hackerskými útokmi alebo krádežou údajov. Najdôležitejšími aspektmi bezpečnosti digitálnych údajov sú **dôvernosť**, **integrita** a **dostupnosť**, ako aj **autentickosť** a **záväznosť**. Údaje sú v bezpečí vtedy, keď sú zabezpečené aj spomenuté prvky.

Pokusy o ich narušenie sa nazývajú **počítačová kriminalita**. Môže ísť o pokusy o podvod, zachytenie alebo sledovanie údajov, ale aj o sabotáž počítačových systémov. V tomto kontexte je dôležité kľúčové slovo „hacking“. Ide o pokus získať **nezákonný a neoprávnený prístup do počítačových systémov alebo sietí**. Patrí sem aj tzv. e-mailový phishing, pri ktorom sa posielajú falošné e-maily s cieľom oklamať príjemcu a donútiť ho, aby niekam **zadal svoje osobné alebo pracovné údaje** (prístupové údaje alebo heslá atď.).

Údaje sa dajú ukradnúť aj inak ako cez internet, a preto ich **treba aj fyzicky zabezpečiť proti neoprávnenému prístupu alebo krádeži**. Na to existujú rôzne metódy, ako napríklad heslá, uzamknutie miestností s hardvérom, nastavenie zvukových výstražných signálov alebo dokonca mikrobodky M-DotDNA pripojené k mobilným zariadeniam.

Na spracovanie, analýzu a prezentáciu údajov nám Excel, najznámejší **tabuľkový program**, poskytuje širokú škálu funkcií. **Matematické** aj **štatistické funkcie** nám pomáhajú spájať údaje. **Grafy** nám umožňujú graficky zobraziť vzťahy medzi jednotlivými údajmi. Pomocou **kontingenčných tabuliek** možno pomocou filtrov a ďalších nástrojov na analýzu údajov štruktúrovať, analyzovať a vyhodnocovať aj veľmi veľké množstvo údajov.

Každý, kto organizuje online stretnutia, musí ovládať príslušný softvér. Spomenieme dva dôležité – **Microsoft Teams** a **Zoom**. Microsoft Teams ako súčasť komplexného softvérového balíka je v rámci **komplexnej online spolupráce vhodný najmä pre väčšie spoločnosti**. Zoom je **prístupnejší**, a preto sa hodí napríklad na externé stretnutia. Digitálny priestor je verejným priestorom, preto je potrebné aj tu dodržiavať **niektoré dôležité zásady slušného správania**.

Pri prezentovaní je na jednej strane dôležité zachovať si **profesionálny vzhľad** (aj pri online schôdzkach) – k tomu prispieva vhodný jazyk (aj reč tela), príprava a upravený zovňajšok. Na druhej strane vám **nástroje, ako je prezentačný a interaktívny softvér**, pomôžu atraktívnym spôsobom usporiadať a predstaviť obsah poslucháčom. Dbajte na to, aby ste **technické pomôcky používali rozumne, teda iba ako doplnok k hovorenému prejavu**. Vždy buďte pripravení na to, že v prípade technických problémov budete musieť prezentovať aj bez technických pomôcok.

1.6 Zdroje:

Microsoft Support: Basics tasks in Excel. https://support.microsoft.com/en-us/office/basic-tasks-in-excel-dc775dd1-fa52-430f-9c3c-d998d1735fca

Excel Easy: Basics. https://www.excel-easy.com/basics.html

Digital Guide IONOS: E-Mail Sicherheit. https://www.ionos.at/digitalguide/e-mail/e-mail-sicherheit/wie-man-spam-mails-erkennt-und-ihnen-vorbeugt/

Bundesamt für Sicherheit und Informationstechnik: Spam – zwielichtige E-Mails und Falschmeldungen. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Spam/spam.html

Varonis: Data Security: Definition, Explanation and Guide. https://www.varonis.com/blog/data-security

Kaspersky: What is hacking? And how to prevent it. https://www.kaspersky.com/resource-center/definitions/what-is-hacking

Gesellschaft für Informatik: Informationen und Daten. https://informatikstandards.de/standards/inhaltsbereiche/information-und-daten

Zoom: Wie unterscheidet sich Zoom von Microsoft Teams? https://explore.zoom.us/de/zoom-vs-microsoft-teams/

AvePoint: Microsoft Teams vs. Zoom: Welches Ist das beste Tool für die Zusammenarbeit?

Magazin oft the society of women engineers: Digital Body Language: How to Build Trust and Connection, No Matter the Distance. https://magazine.swe.org/media-spring-22/

bit academy

CAR Master training

GRATULUJEME K DOKONČENIU TEJTO VZDELÁVACEJ JEDNOTKY!

MÁTE ZÁUJEM O ĎALŠIE INFORMÁCIE?

TEŠÍME SA NA VAŠU NÁVŠTEVU NAŠEJ WEBOVEJ STRÁNKY!

EuroProfis

bit schulungscenter member of bit group

DANMAR COMPUTERS IT matters

IHK IHK-Projektgesellschaft mbH OSTBRANDENBURG

FEMEVAL Federación Empresarial Metalúrgica Valenciana

bit schulungscenter member of bit group

Co-funded by the European Union

Financované Európskou úniou. Vyjadrené názory a názory sú však len názormi autora (autorov) a nemusia nevyhnutne odrážať názory Európskej únie alebo Európskej výkonnej agentúry pre vzdelávanie a kultúru (EACEA). Európska únia ani agentúra EACEA za ne nemôžu niesť zodpovednosť.