Testo
Whitepaper
S Wi-Fi do Cloudu

Be sure. testo

Bezdrátový přenos
s Wi-Fi do Cloudu.

www.testo.cz

Krátké shrnutí.

Cloud (též nazývané Cloud-Computing) popisuje poskytnutí infrastruktury IT jako třeba místo v paměti nebo softwaru přes internet. To pro jednotlivé uživatele znamená, že se nemusí pro řešení Cloud vlastnit žádný vlastní server nebo instalovat software na lokálním PC. Podle požadavků existují různé modely Cloudu, které se liší rozsahem výkonu a bezpečností dat. Které přesně, se dozvíte na této stránce.

Největší výhoda Cloudu spočívá v jeho flexibilitě, protože je možné služby podle potřeby měnit. Navíc je přístup k datům v Cloudu možný odkudkoliv a pomocí jakéhokoliv přístroje s přístupem na internet. Flexibilní přístup na Cloud je možný, díky konvenční technologii WiFi.

Ohledně kódování, šifrování dat a zajištění sítí WLAN však existuje něco, na co je třeba dbát.

Tento Whitepaper se zabývá důležitými standardy a relevantními bezpečnostními informacemi.

Obsah.

Krátké shrnutí **02**
Obsah **03**
Co je Cloud? **04**
Úrovně služeb Cloudu **05**

Různé modely Cloudu **06**
Komunikační a rádiové standardy. **06**
Bezpečnost v rádiové síti. **08**

Závěr **10**

O autorovi. **11**
Další Whitepaper pro Vás ke stažení. **11**
Testo: High-Tech ze Schwarzwaldu. **12**

Co je Cloud?

S pojmem „Cloud“ se dnes setkáváme všude a proto se zdá, že je velmi nový. V informační technologii však byl již na začátku devadesátých let vytvořen jako symbol pro počítačové sítě, jejíž skutečná fyzikální struktura nebo způsob fungování je pro uživatele nedůležitá, vůči němu se však jeví jako standardní počítač.

Velkou výhodou oproti klasickému počítači na Vašem stole nebo pod ním je, že Cloud-Computer roste flexibilně se svými zadáními – kapacita paměti, operační paměť a procesory je možné libovolně rozšiřovat (škálovat).

Přitom však pojem „Cloud“ vůbec nic neříká o tom, kde se tento Cloud-Computer nachází. Stejně tak jako existují auta k pronájmu nebo na leasing, je možné si zatím kapacitu počítače pronajmout nebo pořídit na leasing. Tyto počítače navíc už nemusí být nutně ve vlastním výpočetním středisku, ale mohou být provozovány na jiném, libovolném místě. Musí pouze existovat připojení k síti. Internet se používá jako datový okruh a proto se často dává do přímého porovnání s Cloudem. Přes internet máme zatím téměř všichni více nebo méně pravidelný kontakt s Cloud-Computery, aniž bychom si toho byli nezbytně vědomi, jako například internetové online bankovnictví, průběhy objednávek u zásilkových obchodů, účet u poskytovatele e-mailové schránky nebo sociální média – všechny tyto každodenní procesy by nebyly bez aktuálního Cloudu na pozadí myslitelné.

Zvláště praktické jsou Cloudové aplikace k ukládání dat, především tehdy, mají-li být tato data využívána různými osobami nebo má-li přístup k nim probíhat z různých míst. Pro některé uživatele by mohlo být důležitým argumentem pro využívání úložiště Cloud také automatické zálohování, aby tak zabránili ztrátě dat z vlastního pevného disku v případě výpadku.

Pro provoz Cloudu je nezbytná sladěná infrastruktura. Ta může být velmi rozsáhlá, aby např. velký zásilkový obchod mohl ve vánočním období zpracovat všechny poptávky. Pro normální dny během roku je tento „Computer“ zcela předimenzován. Co by mohlo být lepší, než tyto zdroje využít potom pro další úkoly a podělit se s ostatními? Je to jen malý krůček k obchodnímu modelu od pouhého provozování Cloudu s distribucí kapacity, které je k dispozici, pro mnoho zákazníků, jak to například dělají poskytovatelé e-mailu a sociálních sítí. Financování infrastruktury probíhá buď přes pravidelnou platbu za využívání, nebo přes poskytnutí osobních informací, které mají finanční hodnotu, jako například u sociálních médií.

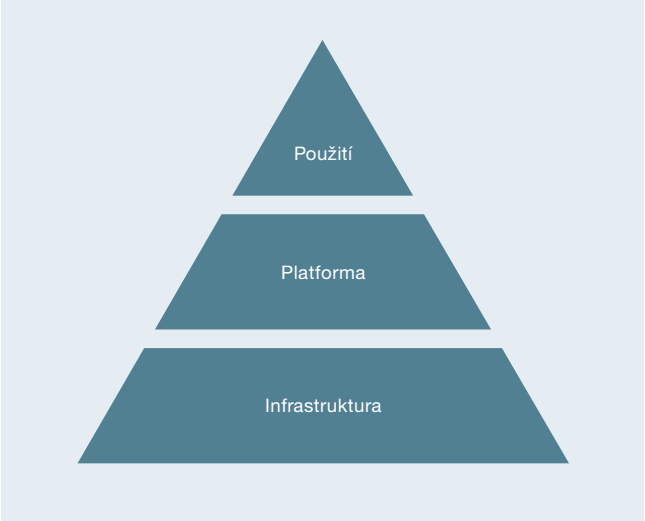
Úrovně Cloudových služeb.

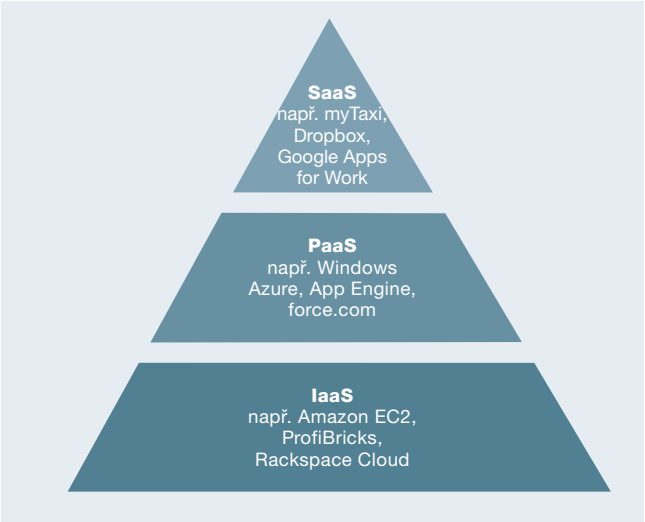
Cloudové služby jsou v zásadě nabízeny ve třech různých úrovních, které se liší rozsahem poskytovaných zdrojů.

Služba infrastruktura (IaaS)
Místo nákupu infrastruktury IT se tato v případě potřeby pronajímá, není tedy potřeba vstupní investice. Tím je možné v krátké době reagovat na změny požadavků infrastruktury IT. O kompletní administraci provozních systémů a aplikací se stará zákazník sám.

Služba platforma (PaaS)
Tento model jde o krok dále a dává k dispozici kompletní prováděcí prostředí spolu s podřízeným hardwarem a softwarem, na němž může zákazník rozvíjet a provozovat svoje vlastní aplikace. Potřebný výkon počítače a potřebu kapacity paměti je možné dle potřeby upravovat.

Služba software (SaaS)
V tomto balíčku, který nevyžaduje žádnou péči, jsou dány k dispozici infrastruktura, platforma a potřebné aplikace. Přístup k aplikacím probíhá zpravidla přes internetový prohlížeč a je proto nezávislý na použité platformě uživatele servisu. Pro používání a provoz se platí poplatek za používání. Poskytovatel služby za to přebírá pořizovací a provozní náklady, mimo jiné za kompletní administraci IT, práce na údržbě, aktualizace a zálohování.





Cloud-Computing: Třístupňový model

Různé modely Cloudu.

Cloud-Computing je v podstatě nabízen v následujících modelech, které se řídí podle aktuálních požadavků zákazníků na zabezpečení.

Veřejný Cloud
Veřejný Cloud nabízí přístup do IT infrastruktury široké veřejnosti přes internet. Zákazníci si infrastrukturu dělí a platí za to zpravidla na základě skutečného využití. Nemají žádné výdaje za počítačovou a datovou infrastrukturu.

Soukromý Cloud
Soukromý Cloud je infrastruktura, je provozována výlučně pro jednu osobu, firmu nebo organizaci. Přitom může probíhat provoz tohoto Cloudu jak interně (prostřednictvím vlastního výpočetního střediska – lokálně), tak také externě prostřednictvím poskytovatele služby.

Komunitní Cloud
Komunitní Cloud je zvláštní forma soukromého Cloudu, která je provozována pro omezený okruh uživatelů, který může být prostorově rozdělen, jako např. městské úřady, univerzity nebo výzkumné společnosti.

Virtualní soukromý Cloud
Virtuální soukromý Cloud je oblast izolovaná bezpečnostními opatřeními v infrastruktuře, která je principiálně dosažitelná jako veřejný Cloud.

Komunikační a rádiové standardy.

Všechny nabídky Cloudu potřebují datové propojení k zákazníkovi. Je-li připojení přes internet, je přiměřeně komfortní a nabízejí se četné možnosti přístupu.

Bezdrátové připojení z přístrojů, jako jsou notebooky, tablety a chytré telefony, k internetu probíhá buď přes data mobilní telefonní sítě nebo přes síť WLAN. Tyto Wireless Local Area Networks jsou lokání rádiové sítě, které vycházejí z mezinárodního standardu a mají dosah do 100 m. V centru takové rádiové sítě WLAN stojí Access-Point (přístupový bod), který rádiové propojení WLAN vede dále do internetu buď pomocí kabelu nebo mobilní rádiové sítě. Často jsou tyto přístupové body nazývány tako (Wi-Fi)-Hotspots.

Protokol IEEE 802.11
K tomu, aby chytré telefony, tablety a ostatní přístroje, které byly vyvinuty v rámci Internetu věcí (IoT), mohly tuto techniku všude využívat, jsou zapotřebí standardy pro rádiová spojení.

V roce 1990 začala pracovní skupina IEEE pracovat na standardu pro bezdrátové sítě. Institute of Electrical and Electronics Engineers je celosvětový profesní svaz inženýrů hlavně z oborů elektrotechniky a informační techniky. Vyvinul protokol a metodu přenosu pro bezdrátové sítě. Protokolu standardu IEEE 802.11 etablovanému v roce 1997 se dostalo rychlého přijetí a rozšíření. Následným budováním byl tento standard běžně rozšiřován a zlepšován. Tato rozšíření se rozeznávají podle připojených malých písmen jako např. a, b, g, n.

Jelikož pásmo 2,4 GHz smí být ve většině zemí využíváno bez licence, tak se přístroje podle standardů 802.11b/g rychle rozšířily. Aktuálně se využívají i další frekvenční pásma: standard 802.11ac využívá pásmo 5 GHz, s 802.11ad pásmo 60 GHz a 802.11ah je připravena pro pásmo 900 MHz .

Nejdůležitější rádiové frekvence.

2,4-GHz:

Výhody

- Překoná clonící materiály s nižšími ztrátami - větší dosah
- Bezpoplatkové, sdílené frekvenční pásmo ISM
- Velké rozšíření, nízké náklady na přístroje

Nevýhody

- Frekvenční pásmo se musí dělit s ostatními přístroji, příp. radiotechnikou (mj. Bluetooth, mikrovlnné trouby, dětské chůvičky, bezdrátové telefony), s tím jsou spojené poruchy a interference
- Bezporuchový provoz na stejném místě je možný pouze maximálně u 4 sítí (USA: 3), protože efektivně jsou k dispozici pouze 4 (téměř se překrývající) kanály (v Německu: kanály 1, 5, 9 a 13 – v USA 1, 6 a 11)

Pásmo 5-GHz

Výhody

- Zřetelně vyšší přenosová rychlost
- Méně využívané frekvenční pásmo - méně poruchový provoz
- Větší dosah, jelikož je s 802.11h možný vysílací výkon až 1000 mW – to nadměrně kompenzuje větší tlumení vyšších frekvencí

Nevýhody

- Silnější regulace v Evropě: na většině kanálů je zapotřebí dynamická selekce frekvence (DFS) aby např. nebyly rušeny meteorologické radarové systémy; na některých kanálech není dovolen provoz na volném prostranství; pokud není využívána automatická kontrola vysílacího výkonu (TPC-Transmit Power Control), musí být vysílací výkon redukován
- Signál je rychle stíněný zdmi

Obecně umožňují použité vysoké frekvence vysokou přenosovou rychlost. Podle použitých materiálů jsou však v budovách rádiové vlny silně potlačovány. Má-li být větší budova kompletně pokryta rádiovou sítí, může být proto nezbytné, zřídit buď více Access-Points nebo rozšířit dosah signálu tak zvaným opakovačem signálu WLAN.

Wi-Fi (Alliance)

Tato organizace byla v roce 1999 původně založena pod názvem Wireless Ethernet Compatibility Alliance (WECA) jako spolek výrobců. V roce 2002 se WECA přejmenovala na Wi-Fi Alliance.

Spolek si dal za úkol certifikovat výrobky svých výrobců na bázi standardu protokolu IEEE-802.11 podle vlastních směrnic a zaručit tak spolehlivý provoz mezi různými bezdrátovými přístroji. Tyto výrobky získávají certifikát Wi-Fi a smí proto nést logo „Wi-Fi“. Tím se toto logo Wi-Fi vyvinulo v celosvětové synonymum pro bezdrátovou lokální síť na bázi standardu protokolu IEEE-802.11.
Za odpovídající poplatek se ovšem testují pouze produkty členů spolku. Chybějící logo Wi-Fi na přístroji výrobce, který není členem spolku, nevytváří nutně odchylku od standardu.

Logo Wi-Fi

Bezpečnost v rádiové síti.

Na rozdíl od kabelového propojení mohou být rádiová propojení jednoduše a nepozorovaně odposlouchávána. Pro ochranu privátní sféry musí být propojení šifrována. Dále může být nutné omezit přístup k Access-Point na známé uživatele. Celosvětově existují velmi různé právní názory k odpovědnosti provozovatele Acces-Point se zřetelem na jeho používání.

Přístup k Access-Pointu
Když se vyexpeduje router WLAN, je přednastaveno standardní heslo pro administrátora routeru. To je zpravidla veřejně známé, protože jsou návody k obsluze přístrojů k dispozici i na internetu. Proto je při uvádění do provozu důležité, změnit jak přihlašovací údaje administrátora, tak také k němu příslušné heslo.

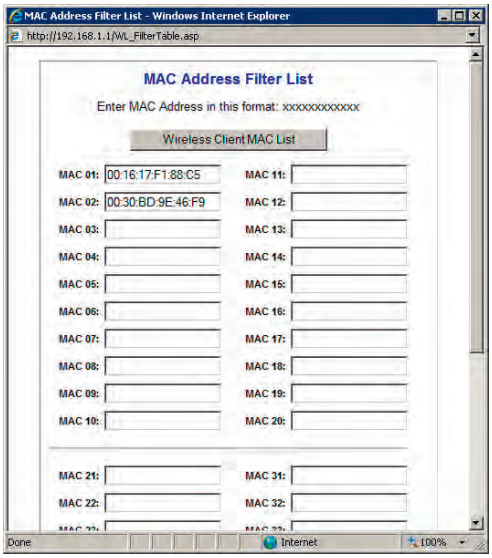
Mnoho routerů nabízí možnost spravovat jej přes internet, přihlásit se a provést administrativní změny. Standardně je tato funkce vypnutá. Neexistují-li žádné závažné důvody pro aktivací této funkce, doporučuje se nechat vzdálenou administraci routeru WLAN deaktivovanou.

Každý Access-Point může nebo by měl mít individuální název, aby jej bylo možné odlišit od ostatních přístupových bodů. Toto jméno sítě (SSID – Service Set Identifier) je zpravidla vysíláno Acces-Pointem a je proto pro všechny potenciální uživatele viditelné. Pokud tento přístupový bod nemá být pro veřejnost viditelný, je možné vysílání SSID na routeru vypnout. Uživatel může mít k němu přesto přístup, pouze musí k tomu znát název sítě a nemůže si jej na svém přístroji vybrat ze seznamu viditelných přístupových bodů.

Typický seznam SSIDs

Volba hesla je další krok ve směru bezpečné WLAN. Na tento bod se stále znovu upozorňuje, přesto existují sítě, jejichž heslo je stejné jako SSID nebo je to snadno uhodnutelný sled čísel.

Další možnost, jak znesnadnit neoprávněné použití Acces-Pointu, je tzv. filtrování adres MAC (Media Access Control). Každý modul WiFi má jednoznačnou MAC adresu, která je uložena v rádiovém modulu jako poznávací signál a je používána k identifikaci v rádiovém provozu. Provozovatel Acces-Pointu může v přístroji uložit seznam MAC adres těch přístrojů, kterým chce dovolit přístup. Pokusy o kontakt ostatních rádiových modulů jsou pak Acces-Pointem odmítnuty.



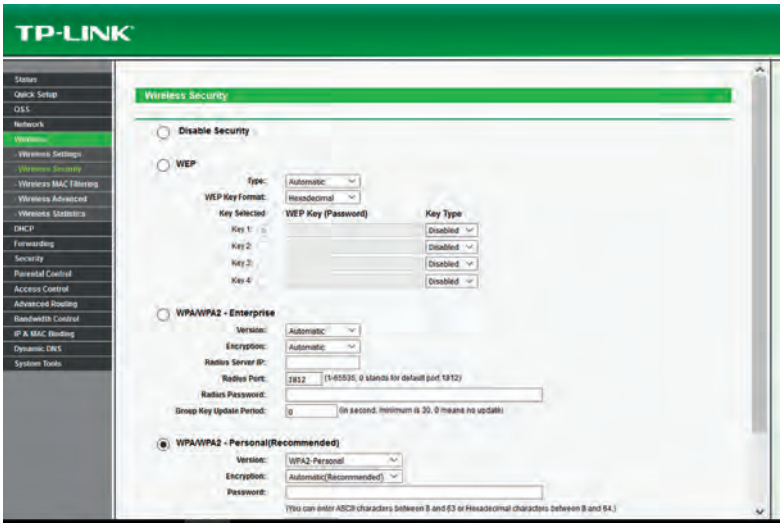
Seznam s povolenými adresami MAC

Šifrování

Další důležitý krok pro zajištění sítě WiFi proti neoprávněnému používání spočívá v šifrování komunikace. Všechny aktuální routery WLAN disponují příslušnými nastaveními. V rámci stále se dále rozšiřujícího používání technologie WLAN byly vyvíjeny stále lepší metody pro šifrovanou komunikaci, protože byla stále znovu odhalována slabá místa a metody tím byly napadnutelné.Pouze kvůli úplnosti zde musí být jmenovány ty metody kódování, které zatím platí jako nespolehlivé a proto by se již neměly používat:

- WEP (Wired Equivalent Privacy)
- WPS (Wi-Fi Protected Setup)
- WPA (Wi-Fi Protected Access)

Aktuální metoda WPA2 (Wi-Fi Protected Access 2) platí jako těžko překonatelná, pokud se použijí též přiměřená bezpečná hesla. Momentální bezpečnostní standard pro rádiové sítě podle standardu WLAN IEEE 802.11a, b, g, n a ac a je založen na standardu Advanced Encryption Standard (AES). Proto by měla být tato metoda momentálně používána.



Možnosti kódování v konfiguraci routeru

Ověřování WLAN

Ne každý smí používat každou WLAN. Přístup k WLAN sice může být omezen heslem. Je-li však jednou heslo oznámeno, je tím nejenom přístup, ale také šifrování nespolehlivé. U větších sítí, např. ve firmách, může mít proto smysl, přiřadit každému uživateli vlastní přístupová data (uživatelské jméno a heslo), která mohou být centrálně spravována. Tato správa se uskutečňuje na speciálním serveru Radius (Remote Authentication Dial-In User Service). Má-li být např. zaměstnanec vyřazen, je nezbytné přístupové heslo pro WLAN změnit. Místo toho naprosto stačí na serveru Radius vymazat příslušná přístupová data.

Závěr.

S Cloud-Computing mohou soukromí uživatelé, firmy a veřejná zařízení profitovat z výkonné infrastruktury IT, aniž by si ji museli sami pořizovat a provozovat. Díky modelu „pronajmout místo kupovat“ zato získají značnou míru flexibility. Na rozdíl od vlastního serveru se dá pronajatá kapacita Cloudu upravovat. Zpravidla se momentálně nabízené modely Cloudu liší velikostí zdrojů poskytovaných nabízejícím a požadovanou bezpečností dat /privátní sférou.

Zatím co data a aplikace v Cloudu (tedy v počítači nebo počítačové síti kdekoliv na světě) se ukládají nebo běží, může zákazník tyto vyvolat kdykoliv a odkudkoliv na světě pomocí téměř libovolného koncového přístroje.
To je rozhodující především v tak zvaném Internetu věcí (IoT). Tento výraz popisuje síťové sdílení nejrůznějších produktů pomocí internetu. V této souvislosti často jmenovaná chladnička, která automaticky objednává mléko, přitom představuje pouze jeden – i když praktický – okrajový jev. Mnohem zajímavější jsou inteligentní výrobní stroje, které mohou automatizovaně objednat materiál nebo záznamníky dat, které měří klimatické podmínky a vyšlou alarm, když dojde k narušení hraničních hodnot.

Cloud se však dá efektivně a komfortně používat pouze přes odpovídající rádiové a komunikační standardy. Nejdůležitější je zde WiFi od WiFi-Alliance. Protože však je možné bezdrátovou komunikaci nebo přenos dat snadněji sledovat nebo ilegálně využívat, doporučuje se řada bezpečnostních opatření. Ta sahají od ochrany heslem přes kódování až po ověřování WLAN pomocí MAC adresy.

Avšak když se člověk po uvážení rozhodne pro vhodné řešení Cloudu a respektuje přitom při propojení dat nejaktuálnější bezpečnostní standardy, nestojí efektivnímu využití této technologie nic v cestě.

O autorovi.

Dr. Volkmar Wismann. Narozen v Hamburgu, promoval v oboru fyziky a elektrotechniky a věnoval se základnímu výzkumu v radiolokaci. Po deseti letech kdy působil jako poradce pro pozorování Země, byl nejdříve činný ve firmě zabývající se záznamníky dat a nyní pracuje na vedoucí pozici u specialistů na měřicí techniku Testo.

Další Whitepaper pro Vás ke stažení:

Záznamníky dat: chytrá alternativa proti termohydrografům.

- Jak přesně měří záznamníky dat?
- Jaké různé modely existují?
- Jaké výhody nabízejí záznamníky dat oproti termohydrografům?
- Kde lze v muzeích, galeriích a archívech záznamníky dat použít?

https://www.testo.com/testo-160

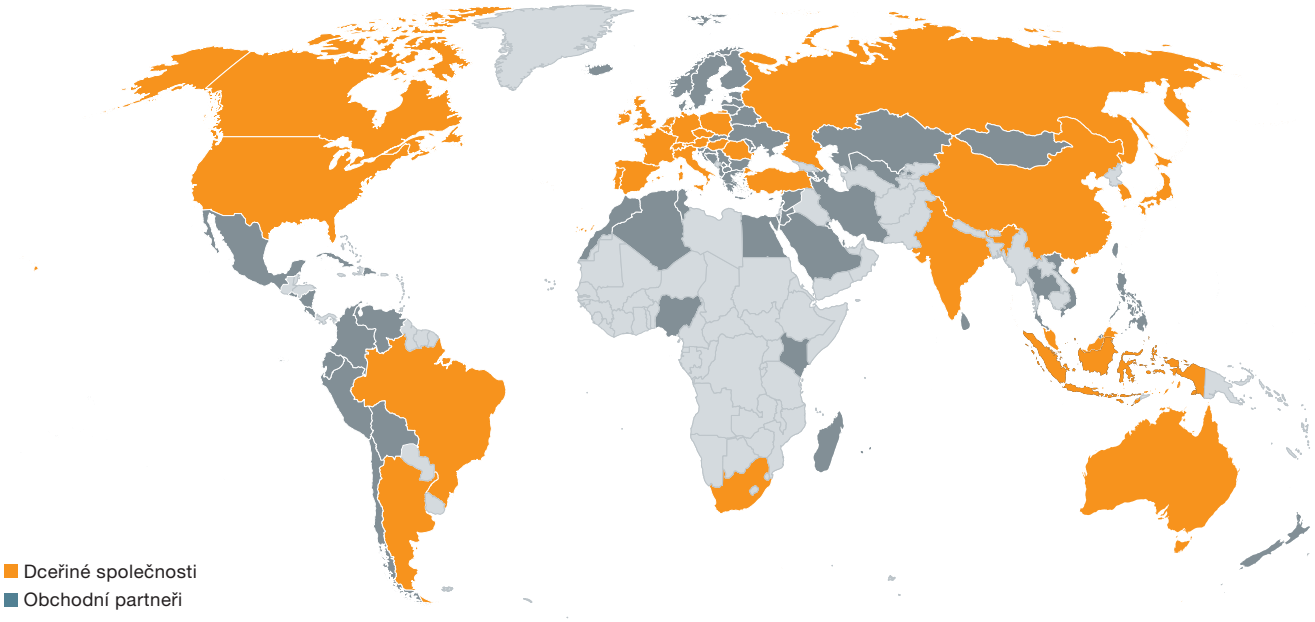
Sledování CO_2 a kvalita vzduchu v místnosti.

- Od jakého množství je kysličník uhličitý pro člověka nebezpečný?
- Jaké hraniční hodnoty existují pro vnitřní prostory?
- Co se dělá s postiženými budovami?
- Jak lze co nejlépe měřit a sledovat CO_2 a kvalitu vzduchu v místnosti?

https://www.testo.com/testo-160

Be sure. testo

Testo: High-Tech ze Schwarzwaldu.



Firma Testo se sídlem v Lenzkirchu ve Schwarzwaldu je na celosvětové špici v oblasti přenosných a stacionárních měřicích přístrojů. 2 700 zaměstnanců ve 33 dceřiných společnostech na zeměkouli zkoumá, vyvíjí, vyrábí a prodává pro high-tech firmu. Expert na měřicí techniku přesvědčuje zákazníky ve světě velmi přesnými měřicími přístroji a inovativními řešeními pro management měřených dat zítřka. Přístroje od firmy Testo pomáhají šetřit čas a přírodní zdroje, chránit životní prostředí a zdraví lidí a zvyšovat kvalitu zboží a služeb.

Průměrný roční nárůst přes 10 % od založení v roce 1957 a aktuální obrat přes čtvrt miliardy Euro zřetelně ukazují, že se Schwarzwald a systémy high-tech k sobě perfektně hodí. K receptu na úspěch firmy Testo patří také nadprůměrné investice do budoucnosti firmy. Testo investuje zhruba jednu desetinu ročního obratu do výzkumu a vývoje.

Více informací na www.testo.cz

Testo, s.r.o.

Jinonická 80
158 00 Praha 5
tel.: 222 266 700
fax: 222 266 748
e-mail: info@testo.cz

www.testo.cz