EJ 01 23

Export Journal

Váš odborný a spolehlivý rádce

Začala nová éra Komerční banky

Počet Bank iD uživatelů roste

Hlavní téma

Nebezpečný život v kyberprostoru?

Úroveň kyberbezpečnosti je v ČR vysoká, říká Ivan Bartoš

Člen představenstva Komerční banky Margus Simson: „Kvalita podvodů roste.“

www.exportjournal.cz

Úvodem

Nepodceňovat kybernetické hrozby

Otázka kyberbezpečnosti nabírá na závažnosti doslova závratným tempem. Tajné služby, NÚKIB a další složky v posledním období stále častěji upozorňují například na kybernetickou špionáž, jejímž výsledkem může být mimo jiné kompromitace citlivých a utajovaných informací. Hrozí také útoky na volební proces anebo úniky dat a ztráta obchodních tajemství, které vedou k oslabení konkurenceschopnosti.

Zůstaneme-li u byznysu, pak je zřejmé, že ve velkém ohrožení jsou zejména malé a střední firmy. Kyberzločinci, kteří už dnes působí ve formě propracovaných organizací, se totiž snaží zasáhnout co největší počet cílů jedním úderem. Fakt, že právě tento typ podniků tvoří celosvětově více než devadesát procent všech firem, jim to usnadňuje. A jak se dočtete v hlavním tématu tohoto vydání Export Journalu, malé a střední společnosti navíc mnohdy nemají dostatečné prostředky na obranu a současně problematiku podceňují. I proto jsme se v článku pokusili shrnout hlavní zásady prevence možného kyberútoku.

Na téma jsme nahlédli z různých úhlů pohledu, například popisujeme, co přináší nová legislativa, která tuto oblast upravuje. Také si budete moci přečíst komentář českého vicepremiéra a ministra pro místní rozvoj Ivana Bartoše, který mj. zmiňuje konkrétní body na poli kyberbezpečnosti, které si v Česku žádají vylepšení. Určitě vás zaujme i rozhovor s členem představenstva a Chief Digital Officerem Komerční banky Margusem Simsonem o tom, co všechno v oblasti kybernetické bezpečnosti banka dělá nebo jak to vypadá s finančně-bezpečnostní gramotností klientů.

Přeji vám podnětné čtení.

David Formánek
člen představenstva KB zodpovědný za korporátní a investiční bankovnictví

Obsah

Digitální svět

Nebezpečný život v kyberprostoru a jak ho zvládat

Každodenní počítačové útoky proti firmám s cílem získat miliony na výkupném, ovlivňování voleb pomocí dezinformací či fake news nebo propagace extrémistických ideologií na sociálních sítích. Demokratické země se musí bránit.

Přesun našich aktivit a vlastně i velké části životů do virtuální reality interaktivního počítačového světa nabírá v poslední době doslova závratné tempo. Jenže stejně rychle, možná dokonce o něco rychleji, se rozvíjí také kybernetická kriminalita. Počítačoví zlosyni už dávno nejsou mladíci v kapucích. Kolem tzv. hackerů se dnes točí obrovský byznys a tito lumpové jsou podle odborníků stále vynalézavější. Například v nedávné debatě Hospodářských novin zaznělo, že kyberútoky zaměřené proti firmám v České republice jsou doslova na denním pořádku, podniky prý o nich neinformují a na výkupném platí miliony.

Hackerství jako byznys

Situaci významně ovlivňuje geopolitické dění, což se samozřejmě dotýká i kybernetické kriminality. Zejména tak, že útočníci jsou stále častěji za provedení útoků placeni hackerskými skupinami, které v určitých případech podporují i některé státy. Například převážnou většinu útoků, jež letos v lednu zaznamenal český Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), měla na svědomí hackerská skupina NoName057. Skupina se hlásí k Rusku a nabízí platby dalším hackerům, útočícím pod jejich vlajkou.

Zatím poslední Zpráva o stavu kybernetické bezpečnosti, jíž vydal NÚKIB a která se týká roku 2021, mimo jiné ukazuje na výrazný meziroční růst počtu tzv. incidentů. Konkrétně jich úřad zaznamenal 157, zatímco v roce 2020 to bylo „jen“ 99. Mezi nejčastější typy kyberútoků patřily phishing, podvodné e-maily a také skenování vnější sítě. Respondenti, kteří byli součástí analýzy, považovali za nejzávažnější typy útoků v roce 2021 phishing, pokusy o zneužití zranitelností a ransomware. Pro úplnější obrázek dodejme, že trend potvrzují i statistiky Policie České republiky. Ta v roce 2021 vyšetřovala necelých deset tisíc kybernetických kriminálních případů, zatímco v roce 2022 už jich byl téměř dvojnásobek, necelých devatenáct tisíc.

Méně než procento odhalených

Stanislav Simandl, výkonný ředitel firmy MyCom Solutions, pro Hospodářské noviny vysvětlil, že hackeři jsou firmy, které pracují na zakázku. A to tak, že vytvoří vlastní viry, koupí databázi zranitelných cílů a na ty pak zaútočí. Jejich snahou je donutit oběti, aby zaplatily výkupné. Úspěšnost vytěžení peněz je podle Simandla kolem šedesáti procent, ovšem podíl útoků, jejichž pachatele se podaří odhalit, přitom nedosahuje ani jednoho procenta.

Aktualita

Generálním ředitelem Société Générale se stal Slawomir Krupa

Na výroční valné hromadě společnosti Société Générale, která proběhla 23. května 2023, byl novým generálním ředitelem jmenován Slawomir Krupa. Absolvent Institutu d'Études Politiques de Paris má více než 26 let zkušeností v mezinárodním finančním sektoru. Do skupiny Société Générale nastoupil v roce 1996, kariéru zahájil jako inspektor generální inspekce. V roce 1999 ze skupiny odešel a založil start-up v oblasti elektronických financí ve východní Evropě. V roce 2002 se však vrátil, konkrétně do oddělení generální inspekce. O tři roky později se stal členem jeho vedení.

Poté působil v oddělení korporátního a investičního bankovnictví, byl ředitelem pro strategii a rozvoj či zástupcem ředitele pro financování. V lednu 2016 byl jmenován generálním ředitelem SG Americas a o pět let později se stal členem výkonného vedení skupiny jako ředitel globálního bankovnictví a řešení pro investory. Jeho prvním úkolem v pozici generálního ředitele skupiny bude dokončit rozsáhlé probíhající transformace, jako je fúze francouzských sítí, akvizice LeasePlanu společností ALD, expanze Boursoramy a rovněž další rozvoj korporátní a investiční části banky.

Kyberzločinci se intenzivně zaměřují obzvlášť na malé a střední firmy. Jejich snahou je totiž zasáhnout co největší počet cílů jedním úderem. A tak vzhledem k tomu, že malé a střední podniky tvoří celosvětově více než devadesát procent všech firem, zaměřují se především na ně. Navíc tyto společnosti mnohdy nemají dostatečné prostředky na obranu.

Trestuhodné podceňování

Zranitelnost tuzemských firem je podle odborníků mnohdy důsledkem toho, že nemají ani základní strategii pro kybernetickou bezpečnost a také, což s tím samozřejmě úzce souvisí, podceňují přípravu na útok. Tedy hlavně to, aby i po něm dokázaly rychle obnovit dodávky svých produktů a služeb a obecně věděly, co dělat a jak se chovat. Nejjednodušší cestou dovnitř firmy bývá selhání zaměstnanců. Nemusí to přitom být jejich chyba. Jak poznamenávají analytici slovenské společnosti Eset ve svém e-booku, každý pracovník nemůže být zároveň bezpečnostním expertem.

Export Journal komentuje

Většinu útoků, jež letos v lednu zaznamenal NÚKIB, měla na svědomí hackerská skupina NoName057, která se hlásí k Rusku.

„Útočníci to vědí a používají techniky sociálního inženýrství, které ‚donutí' uživatele kliknout na zákeřný odkaz ve spamu nebo phishingovém e-mailu a navštívit škodlivé webové stránky," lze se dočíst v brožuře. Je tedy zřejmé, že jednou z nejdůležitějších věcí, pokud jde o prevenci, je vzdělávání zaměstnanců, mj. pořádání pravidelných školení o bezpečnostní problematice apod. (Podrobnější informace o tom, jak odborníci doporučují kyberútokům předcházet, si můžete přečíst v boxu.)

Problém je ale pochopitelně komplexnější, nelze jen vinit představitele firem z toho, že nebezpečí podceňují. Jak ukazuje průzkum společnosti Sophos z letošního ledna, mezi největší problémy při zajišťování digitální ochrany v českých firmách patří vysoké náklady na pořízení bezpečnostního řešení (myslí si to víc než polovina respondentů), dále je to nedostatek času na implementaci (34 %) a nedostatek kvalifikovaných zaměstnanců (28 %). Analytici Sophosu ovšem také upozorňují na to, že pokud jde o výši nákladů, třeba vedoucí pracovníci v polských nebo maďarských firmách to jako problém tak často nezmiňují. Průzkum Sophosu rovněž ukazuje, že víc než polovina, téměř 60 % českých manažerů, neabsolvovala žádné školení v oblasti kybernetické bezpečnosti.

Povinné osoby se nově budou hlásit samy

Dohánět překotný vývoj v kybernetickém světě a co nejvíc zločincům jejich aktivity ztěžovat, o to se pokoušejí také zákonodárci. Před časem byla schválena evropská směrnice NIS2, která stanovuje řadu pravidel pro tuto oblast a přináší mnohé změny. Ty v České republice nastanou současně s účinností nového zákona o kybernetické bezpečnosti, což by podle plánu mělo být ve druhé polovině příštího roku. (Otázkou ovšem je, jestli je to zvládnutelné. Návrh zákona totiž v připomínkovém řízení údajně „nasbíral" zhruba tisíc připomínek, takže jejich zapracování nejspíš nebude zrovna rychlé.)

Směrnice NIS2 zjednodušeně řečeno označuje kritické sektory a stanoví minimální úroveň kybernetického zabezpečení proti útokům. Přičemž její znění významně rozšiřuje okruh organizací, na které se vztahuje, a navíc, jak upozorňuje advokát Tomáš Ščerba, přináší úplně nový princip tzv. sebeidentifikace. Co to znamená? Tomáš Ščerba vysvětluje, že pokud vaše organizace splňuje kritéria tzv. povinných osob uvedená ve směrnici, automaticky vám vzniká řada povinností, včetně například registrace na portálu NÚKIB. Nemůžete proto ve většině případů čekat na to, až a popřípadě jestli příslušné kroky zahájí úřad.

Fake news, řetězové e-maily a další radosti

Problematiku kybernetické bezpečnosti je nepochybně potřeba vnímat šířeji a zahrnout do ní například i odolnost proti působení dezinformací, fake news, řetězových e-mailů apod., jejichž původci se snaží o narušení sociální soudržnosti a demokratického systému v České republice a dalších zemích. Stačí si vybavit pár situací z poslední doby. Třeba výrazný nárůst dezinformační aktivity na sociálních sítích, digitálních platformách či v řetězových e-mailech po prvním kole letošních prezidentských voleb v Česku. Byla zaměřena proti současné hlavě státu Petru Pavlovi. Nebo tisíce Čechů, kteří na sociální síti Telegram sledují účty propagující krajně pravicové a konspirační ideologie, například o nadřazenosti Slovanů apod. Popřípadě fakt, že v České republice klesá počet středoškoláků, kteří považují nezávislá média za důležitá pro fungující demokracii.

Že situaci v žádném případě nelze brát na lehkou váhu dokazuje také působení mezinárodní skupiny nazvané „Team Jorge", která stojí za dezinformačními kampaněmi po celém světě. Skupina, které byla před třemi měsíci odhalena v rámci tajného vyšetřování, prodávala hackerské služby a přístup k obrovské armádě falešných profilů na sociálních sítích. Jak uvedl deník The Guardian, její mozek – Tal Hanan, padesátiletý bývalý příslušník izraelských speciálních jednotek, který pracuje pod pseudonymem „Jorge" – podle všeho už víc než dvě desetiletí působí v utajení v rámci voleb v různých zemích. On sám tvrdí, že byl zapojený do víc než třiceti prezidentských voleb. Z těchto a dalších signálů je zřejmé, že demokratické společnosti se musí tvrdě bránit. Jenže česká vláda zatím pouze po krátké době ve funkci propustila zmocněnce pro oblast médií a dezinformací, Michala Klímu, aniž by cokoli mohl předložit. A poté jmenovala svým poradcem pro národní bezpečnost Tomáše Pojara, náměstka ministra zahraničí pro evropské záležitosti, který prohlásil, že neumí definovat, co je dezinformace. Tato blamáž zatím příliš nadějí do budoucnosti, kterou může dezinformační svět nenávratně poškodit, nevzbuzuje.

Jak ve firmách předcházet kybernebezpečí

Analyzujte možná rizika a vytvořte bezpečnostní strategii
Je třeba si ujasnit, co chcete nebo musíte chránit. Primárně je důležité zabývat se aktivy, jež jsou připojená na internet. Dále zabezpečit síť a přístup k systémům, klasifikovat veškerá data, ta citlivá pak šifrovat, zajistit zálohu důležitých údajů atp. V první řadě ale přiřaďte odpovědnost za tuto agendu konkrétní osobě.

Vytvořte plány, co dělat v případě útoku
Vaše organizace by měla být schopná pokračovat v dodávkách produktů a služeb i po bezpečnostním incidentu. Budete-li mít plán, jak po útoku co nejrychleji obnovit provoz, nebudete také donuceni platit výkupné.

Útok nahlaste Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB)
Ten vám v případě potřeby může účinně pomoci, případně i vyslat na místo tzv. tým rychlé reakce.

Zásadně neplaťte výkupné
Pokud vyděrači zjistí, že jste ochotni platit, můžete se snadno stát obětí dalšího vydírání. Navíc neexistuje žádný postup, jak takové výdaje vykázat v účetnictví.

Vzdělávejte své zaměstnance
Je třeba členy vašich týmů pravidelně školit, protože se jasně ukazuje, že pro kyberzločince vede nejjednodušší cesta dovnitř firmy právě přes zaměstnance, kteří mohou snadno podlehnout nějaké formě manipulace. Navíc často na sebe i na firmu nevědomky upozorní, třeba na sociálních sítích.

Rozhovor čísla

„Kvalita“ podvodů roste. Technologie ztěžují rozlišení pravdy od lži, říká Margus Simson

Člena představenstva Komerční banky Marguse Simsona, který je také jejím Chief Digital Officerem, jsme se zeptali, co všechno banka v oblasti kybernetické bezpečnosti dělá nebo jak to vypadá s finančně-bezpečnostní gramotností jejích klientů.

Jak se v meziročním srovnání vyvíjí počet kyberútoků na Komerční banku? A je možné říct třeba i to, kolik peněz klientů jste ochránili?
Počítání kybernetických útoků je vždy trochu komplikované, protože tu spoustu malých útoků, k nimž dochází neustále, obvykle eliminuje naše automatická obrana. Závažnější pokusy o proniknutí a útoky typu odepření služby pak zažíváme zřídka. Celkově počet preventivních akcí, které provádíme, meziročně vzrostl přibližně o 50 %, ale množství zjištěných událostí zůstalo většinou stejné. Vyjádřit to vše v penězích je také obtížné. Jelikož jsme byznys založený na důvěře, pak to, že zabráníme pokusu o narušení, má spíše nevyčíslitelnou hodnotu. Jak pro banku, tak pro klienty.

Změnilo se v této věci něco v důsledku častějšího využívání bankovní identity?
Zatím ne. Každá nová technologie, kterou používáme, potenciálně zvyšuje rizika, protože se objevují nové příležitosti k nalezení nových slabých míst. Ovšem pokud by klienti více využívali BankID, z dlouhodobého hlediska by podle mého názoru rizika spíše poklesla. Protože s tím, jak by si zákazníci zvykli používat jedno řešení, došlo by k omezení možností pro spáchání podvodu. Používání služby BankID je však zatím spíše na začátku.

Útočníci jsou stále sofistikovanější. Co to pro vás znamená, jaké nové bezpečnostní prvky jste například byli v Komerční bance nuceni zavést?
Udělali jsme toho hodně. Nejviditelnější změnou pro uživatele je plošné používání dvoufaktorové autentizace. Ovšem současně jsme – a to klienti nevidí – pilně pracovali na segmentaci sítě, abychom tak hackerům v případě úspěšného průniku ztížili přechod ze serveru na server. Také jsme prováděli penetrační testy pro každou aplikaci, která je připojena k internetu, či pracovali na snížení potenciálu úniku dat. Provádíme také tzv. cvičení Red Team, tedy zkoušíme útočit na vlastní systémy, abychom našli jejich případná slabá místa. Seznam těchto aktivit je velmi dlouhý.

Jak byste popsal nedávný vývoj v této oblasti z hlediska přístupu vašich klientů, a to jak jednotlivců, tak i firem? Zlepšuje se jejich finančně-bezpečnostní gramotnost?
Ano, povědomí zákazníků o zásadách bezpečnosti se každým rokem zlepšuje. Špatnou zprávou ale je, že se zločinci a sofistikovanost jejich útoků vyvíjí stejně rychle. Celkově vzato, z hlediska zajištění peněz uživatel vždy byl a stále je nejslabším místem. Lidé se stávají oběťmi podvodů, které je stále těžší a těžší jako podvody identifikovat. Staly se totiž mnohem osobnějšími, zločinci používají širší škálu postupů a využití nových technologií umožnilo dělat falešné věci tak realisticky, že je těžké rozlišit lež od pravdy. To vše nutí uživatele neustále se o kybernetických hrozbách učit. Je ovšem zřejmé, že to pro lidi v jejich každodenním životě není to nejdůležitější.

Někteří odborníci také říkají, že se útočníci v posledních letech zaměřili na bankovní klienty, a ne tolik na samotné banky. A že lze v této souvislosti mluvit o společenské úloze bank, které by se měly zasadit o to, aby jejich klienti svým chováním neohrozili bezpečnost vlastních peněz. Souhlasíte s tím?
Je samozřejmě pravda, že samotné banky je mnohem těžší napadnout, a proto se zločinci zaměřují spíše na jednotlivé uživatele. Snažíme se proto naše uživatele v oblasti kybernetických hrozeb vzdělávat, jak jen je to možné. Neustále o nich mluvíme, na naší domovské internetové stránce kb.cz zveřejňujeme varování a kybernetické rady, systematicky analyzujeme transakce, abychom porozuměli potenciálně podvodným transakcím, omezujeme uživatelům možnost provádět transakce, pokud cítíme, že hrozba existuje, vyvíjíme nové funkce, které uživateli umožní zvýšit úroveň zabezpečení a porozumět novým možnostem. Jenže pokud člověk převede osobě, s níž si chatoval a která ho požádala o pomoc, velkou částku peněz a nakonec se ukáže, že to byl zločinec, pak stejně nemůžeme dělat nic.

Jaký je postup v případě, že klient banky přijde v důsledku kyberútoku na banku o své peníze?
Kybernetický útok proti bance se obvykle nezaměřuje na peníze konkrétního uživatele, ale spíše na výkupné při útoku ransomwaru. Pokud je napaden konkrétní zákazník, pak se útočníci zaměřují na uživatele, jeho autentizační nástroje, zkoušejí sociální inženýrství, podvody atd. Je-li napaden konkrétní uživatel, pak se případ vyšetřuje ve spolupráci s policií, aby se zjistilo, co a proč se skutečně stalo, čí je to vina a jaké jsou možnosti získání peněz zpět. Banka k těmto situacím vždy přistupuje s maximální pozorností, aby zákazníkovi pomohla dostat zpět své peníze. Ale protože každý útok je poněkud jiný, pak je těžké dát jeden konkrétní recept, jak to bude vypadat příště.

Margus Simson

Od ledna 2019 je členem představenstva a Chief Digital Officerem Komerční banky. Řídí problematiku digitalizace, IT, data managementu a souvisejících oblastí. V průběhu své kariéry pomohl realizovat digitální řešení pro tři největší banky v Estonsku a řadu významných pobaltských firem.

Vícestupňový systém zabezpečení

„Systém ochrany platebních transakcí je výsledkem několika kroků,“ vysvětluje Jan Seifert, Chief Risk Officer Komerční banky. Předně, banky dodržují směrnici PSD2, v jejímž rámci se musí klient mj. prokázat minimálně dvoufázovým ověřením. Dále je to vzdělávání klientů a také jejich informování o aktuálních hrozbách, protože, jak konstatuje Jan Seifert, nejslabším prvkem v celém zabezpečení je uživatel, který často v rámci sociálního inženýrství předá své citlivé údaje útočníkům. Komerční banka rovněž soustavně zvyšuje zabezpečení přístupu do online bankovnictví přidáváním bezpečnostních prvků, jako je např. technologie Cronto kódu. A v neposlední řadě je pak každá platební transakce validována tzv. Fraud Detection System, který využívá nejmodernějších technologií, statistických metod a dalších bankovních informací.

Bezpečnost kybernetického prostoru

Svět zvyšuje investice do kyberbezpečnosti. Přináší to nové možnosti pro exportéry

Kyberbezpečnost jako technologický obor se v posledních letech ze zcela zřejmých důvodů rozvíjí přímo raketovou rychlostí a současně s ní pochopitelně i související technické obory. Proto jsme se rozhlédli po světě a zjišťovali, jaké zajímavé příležitosti se v současnosti českým vývozcům v těchto oblastech nabízejí.

A začněme zemí galského kohouta. Na podzim, konkrétně na říjen, je tam naplánovaná zajímavá podnikatelská mise, při které budou firmy prezentovat inovativní technologická řešení pro větší korporátní struktury. Jak vysvětluje Jakub Smetana, vedoucí zahraniční kanceláře CzechTrade Francie, české firmy tu budou mít příležitost představit svá řešení například v oblasti venture building (čili zřizování nových byznysových možností v rámci korporátních struktur), dále v oblasti inteligentních řešení pro vyplácení mezd (jde například o platformu, která bude umožňovat zaměstnancům vybírat peníze za již odpracované hodiny) nebo také vytváření virtuálních kanceláří a prostor pro práci na dálku.

Jakub Smetana zároveň upozorňuje i na projekty, které skýtají českým exportérům plno zajímavých veřejných zakázek a dalších šancí. Například v rámci plánu „Francie 2030“ byly ohlášeny velké investice do posilování kybernetické bezpečnosti a s tím spojených technologií, přibližně v rozsahu 39 miliard eur. I proto, že byla v nedávné minulosti nucena častokrát čelit kyberútokům na tamní nemocnice. „Obecně proto doporučuji sledovat veřejné zakázky z tohoto odvětví nebo se napojovat na systémové integrátory zde v zemi a skrze ně do veřejných zakázek pronikat. Naše zahraniční kancelář je samozřejmě schopna tyto kontakty českým firmám poskytnout v rámci svých služeb,“ doplňuje šéf CzechTrade Francie.

A upozorňuje také na zajímavou platformu Campus Cyber, kterou založil prezident Emmanuel Macron. Jejím smyslem je sdružovat hlavní aktéry z dané oblasti, pro české firmy by tedy mohlo být zajímavé s kampusem spolupracovat, popř. se stát jeho členy.

Konference a možnosti v akcelerátorech Beneluxu

Mnoho zajímavého se děje v oblasti Beneluxu. Například letos v březnu zamířila do nizozemského Haagu, který se stává evropským hlavním městem pro boj s kybernetickým zločinem, mise českých inovativních firem, jejímž cílem bylo nabídnout česká řešení pro kybernetickou bezpečnost.

V Lucemburku se už na konci června v rámci Digital ICT Week, který pořádá Lucemburská obchodní a komora a společnost Farvest, koná globální technologická konference ICT Spring. Jak vysvětluje Adam Jareš, ředitel regionálního centra střední Evropa agentury CzechTrade, jejím cílem je stimulovat digitální transformaci, představit nejnovější technologické trendy a příležitosti růstu zejména pro startupy a malé a střední podniky. „Prostřednictvím konferencí, přednášek a prezentacemi nejnovějších inovací a trendů nabízí ICT Spring účastníkům jedinečnou příležitost prohloubit své digitální znalosti, sledovat dynamický vývoj ve fintech, kybernetické bezpečnosti a ve vesmírných technologiích,“ popisuje Adam Jareš.

Lucembursko nabízí českým firmám také řadu konkrétních projektů. Je to například:

FinTech Accelerator
Projekt s cílem vytvořit digitální platformu města Lucemburku, která zlepší komunikaci a interakci mezi občany, podniky a městskou správou. Mezinárodní společnosti se mohou zúčastnit tím, že nabídnou své odborné znalosti v oblasti vývoje softwaru, analýzy dat a designu uživatelských zkušeností.

Space Tech Accelerator
Tento projekt je zaměřený na rozvoj průmyslu vesmírných technologií v Lucembursku podporou startupů a malých a středních podniků v této oblasti. Mezinárodní společnosti mohou nabídnout odborné znalosti, včetně vývoje softwaru, analýzy dat a hardwarového inženýrství.

eHealth Lucembursko
Jde o rozvoj národní infrastruktury eHealth, včetně elektronických zdravotních záznamů, telemedicíny a mobilních zdravotnických aplikací. Mezinárodní společnosti mají možnost poskytnout odborné znalosti v oblasti vývoje softwaru, kybernetické bezpečnosti a ochrany osobních údajů.

Digitalizace lucemburských železnic
Projekt poskytne šance těm mezinárodním firmám, které mohou poskytnout řešení související s vývojem softwaru, internetem věcí (IoT) a analýzou dat.

Export Journal komentuje

Vlády zemí reagují na rozvoj kybernetické kriminality a české firmy by toho měly využít. Jejich šance na úspěch rozhodně nejsou malé.

Německo: Mise a rozsáhlý výzkumný projekt

CzechTrade Německo chystá pro firmy z oblasti kyberbezpečnosti jednodenní misi ve spolupráci s GK Mnichov, IHK Regensburg a Bavorským klastrem kybernetické bezpečnosti. Hlavním tématem bude změna evropské směrnice NIS2 v oblasti kyberbezpečnosti a také kyberbezpečnost v obranném průmyslu. „V rámci akce pro české účastníky plánujeme seminář, následnou návštěvu Cyber Security Clusteru v Regensburgu a B2B propojení s významnými hráči v regionu," vypočítává Kristýna Kubíčková, ředitelka CzechTrade Německo. A dodává, že účast přislíbili zástupci institucí jako BayernInnovative, IHK Regensburg a Cyber Security Cluster. Přesné datum akce zatím nebylo stanoveno, měla by proběhnout koncem září v Regensburgu.

Čeští exportéři by také měli věnovat pozornost zajímavým projektům v zemi našeho nejvýznamnějšího souseda. Jeden z nich zastřešuje německá Agentura pro inovace v Cybersecurity GmbH (Cyberagentur) a jak Kristýna Kubíčková vysvětluje, jedná se o zatím největší výzkumný projekt v oblasti bezpečnosti umělé inteligence s výzkumem Robust and Secure Machine Learning. Ve vícestupňovém procesu vyjednávání mají být vyvinuty nové přístupy ke zvýšení robustnosti a bezpečnosti různých přístupů AI v oblasti vnitřní a vnější bezpečnosti. Pětiletý výzkumný projekt bude zahrnovat jak základní výzkum, tak vývoj prototypů.

Singapurské cybercally

Ke špičce v oblasti kybernetické bezpečnosti nepochybně patří Singapur. Jeho vláda i soukromé společnosti aktivně investují do výzkumu, vývoje a implementace technologií pro zajištění kybernetické bezpečnosti. I proto se kybernetickou bezpečností intenzivně zabývá také zahraniční kancelář CzechTrade Singapur.

Ta vloni v Singapuru zorganizovala první ročník mise v oblasti kybernetické bezpečnosti, a to v rámci klíčové akce GovWare. Představitelé českých firem měli například možnost zúčastnit se jednání se zástupci významných subjektů, jako je Cyber Security Agency či Association of Information Security Professionals, nebo navštívit singapurské univerzity National University of Singapore a Nanyang Technical University atd.

Ředitel regionálního centra CzechTrade Ladislav Graner upozorňuje, že agentura letos plánuje druhý ročník, který proběhne 17. až 19. října. „Chceme z mise udělat každoroční událost a současně bychom rádi podpořili přeliv aktivit firem přes Singapur, který považujeme za centrum pro další expanzi do zemí jihovýchodní Asie, jako je Indonésie, Filipíny, Vietnam a Thajsko," vysvětluje.

Rovněž v Singapuru samotném mohou vývozci narazit na zajímavé příležitosti. Za zmínku stojí například iniciativa singapurské vládní Agentury pro kybernetickou bezpečnost (The Cyber Security Agency of Singapore) nazvaná The Cybersecurity Industry Call for Innovation. Takzvané cybercally podporují spolupráci mezi společnostmi, které se zabývají kybernetickou bezpečností a koncovými uživateli, a také podporují společný vývoj inovativních řešení kybernetické bezpečnosti.

České firmy, v partnerství s těmi singapurskými, se mohou každoročně ucházet o přibližně desítku těchto cybercallů, přičemž ty letošní jsou očekávané během léta.

Vybrané společnosti mohou získat podporu do výše 1 000 000 singapurských dolarů na dobu až 24 měsíců.

Nová agentura pro kyberbezpečnost v Kolumbii

Na druhou polovinu letošního roku připravuje v oblasti kybernetické bezpečnosti incomingovou misi do Česka také zastupitelský úřad České republiky v kolumbijské Bogotě, a to ve spolupráci s agenturou CzechTrade. Cílem projektu je podle Pavla Eichnera, ředitele zahraniční kanceláře CzechTrade v Kolumbii, mj. poskytnout možnosti prezentace technologických řešení českých firem, a to jak potenciálním koncovým uživatelům, tak kolumbijským obchodním partnerům.

Pavel Eichler rovněž upozornil, že kolumbijská vláda plánuje založit novou agenturu pro kybernetickou bezpečnost na způsob českého NÚKIB, která by se měla nazývat Agencia Nacional de Ciberseguridad. To s sebou přinese velké množství nových projektů, o které se čeští výrobci budou moci ucházet.

Počet Bank iD uživatelů rychle roste

Bank iD je státem uznávaná identifikační metoda, která umožňuje komunikaci se státní správou i soukromými společnostmi, jako jsou zdravotní pojišťovny, obchody, služby nebo pojišťovny. Její používání je velmi snadné, funguje stejně jako přihlašování k internetovému bankovnictví. A odpovídá tomu i stupeň jejího zabezpečení.

To všechno jsou zároveň důvody, proč Bank iD už alespoň jednou využilo 2,5 milionu bankovních klientů, tedy každý třetí dospělý Čech. Před spuštěním platformy komunikovalo se státem online 500 000 občanů, dnes jich je už víc než 5,5 milionu. A jako svůj identifikační prostředek využívá Bank iD 80 procent z nich. Firem zapojených do Bank iD je v současnosti přes 150.

Počítá se s dalším rozvojem bankovní identity, přičemž roli bank je přinášet uživatelský pohled na online služby státu. Konkrétním společným projektem může být např. plánovaná česká eDokladovka, tedy aplikace, díky které by lidé měli mít možnost prokazovat svou totožnost pomocí mobilu, nebo evropský projekt digitální peněženky eWallet. Ta by měla sloužit i k prokazování dalších atributů, např. řidičského oprávnění, zdravotního pojištění či dosaženého vzdělání.

KB má jako první banka v České republice na střeše fotovoltaiku

Komerční banka už před časem oznámila, že chce být do roku 2026 uhlíkově neutrální. A nedávno udělala další krok k dosažení tohoto ambiciózního cíle. Společnost ČEZ ESCO, která se zaměřuje na energeticky úsporná a klimaticky šetrná řešení pro firmy, obce a veřejnou správu, už dokončila instalaci fotovoltaické elektrárny na centrále banky v pražských Stodůlkách. Má více než 200 panelů a ročně vyrobí téměř 100 MWh bezemisní elektřiny. ČEZ ESCO bude také příštích dvacet pět let zajišťovat provoz panelů a budově KB garantovat dodávku elektřiny za smluvenou cenu. Banka bude investici splácet v ceně odebírané elektřiny, výrazně nižší, než kterou v současné době platí za dodávku ze sítě. Po 15letém provozu také může za 1 Kč elektrárnu odkoupit a dále si vyrábět vlastní energii.

Začala nová éra Komerční banky

Zcela nový pohled na bankovnictví. To je podstatou nové éry Komerční banky, kterou nedávno odstartovala spuštěním Nové digitální banky. Co zmíněný nový pohled znamená? KB představila banku, vybudovanou ve spolupráci s klienty a postavenou na společné expertize a nejmodernějších technologických nástrojích. Na zákaznících v centru dění. Na chytrých produktech a službách. Na novém přístupu k obsluze klientů. Mimo jiné tak lze produkty a služby banky sjednat, využívat, měnit a rušit online bez nutnosti návštěvy pobočky nebo podpory Kontaktního centra. A klient je schopen si vše vyřídit sám. Více se tématu věnujeme v rubrice Koktejl na straně 30.

Názor Ivana Bartoše

Úroveň kyberbezpečnosti je v ČR vysoká. Potřebujeme ale zlepšit spolupráci mezi resorty a experty

Prudký rozvoj moderních technologií v posledních letech před nás mimo jiné klade stále důležitější otázky, na které bychom se měli ve vlastním zájmu pokoušet co nejlépe odpovídat. Už proto, že online svět, který nás dnes obklopuje prakticky na každém kroku, má i svá problematická místa. A není jich právě málo.

Jedním z největších nebezpečí je podle mě šíření dezinformací a manipulace veřejného mínění, hrozbou je rovněž ztráta soukromí v důsledku shromažďování mnoha našich osobních dat různými společnostmi a webovými stránkami bez našeho vědomí.

Ovšem nejzranitelnější jsme asi v oblasti kybernetické bezpečnosti. Pachatelé kybernetických útoků totiž neustále přicházejí s novými způsoby a do intenzity a závažnosti útoků se promítá i geopolitická situace. Třeba NÚKIB zaznamenal, že nejvíc útoků v České republice měla v poslední době na svědomí ruská hackerská skupina NoName057. Je potřeba na to rychle reagovat a přijmout opatření k minimalizaci rizika.

Jak být efektivní a nezničit základní principy

Demokratické státy přistupují k boji proti kybernetickým hrozbám z hlediska ochrany lidských práv a svobod. Jde tedy o to, najít správnou rovnováhu, abychom byli dostatečně efektivní a zároveň nepošlapali principy, na kterých stojí naše společenství. V porovnání s autoritářskými režimy, jako je například Čína, mají demokratické státy samozřejmě výhodu větší svobody, otevřenosti a spolupráce s ostatními demokratickými systémy. Jednou z hlavních výzev pak je nedostatek kvalifikovaných kybernetických odborníků nebo třeba podcenění kybernetického zabezpečení klíčových infrastruktur.

Centralizovaná kontrola je něco, čemu se rozhodně chceme vyhnout. Například používání umělé inteligence (AI) ke sledování, rozpoznávání a hodnocení lidí je na evropském kontinentě nepřijatelné. V Evropské unii se teď mimo jiné vytváří první legislativa sui generis, která to bude řešit, jde o tzv. akt o umělé inteligenci. Jeho záměrem je regulace rizikového využívání AI v praxi, akt proto upravuje užívání a vyvíjení systémů AI na vnitřním trhu. Bude zavádět pravidla v oblasti zdravotnictví, dopravy, financování a administrativy s cílem ochrany základních práv a hodnot občanů EU a zajištění bezpečnosti. Samostatnou kapitolou aktu je v podstatě zabránění zneužití umělé inteligence ke sledování lidí a k podprahovým technikám za účelem ovlivňování chování nebo hodnocení chování.

AI? Zajistit ochranu společnosti, a nezůstat pozadu

V této souvislosti bych rád poznamenal, že nedávnou výzvu vědců a dalších osobností k pozastavení vývoje AI považuji za oprávněnou, protože rizika velmi prudkého vývoje digitálních nástrojů je nepochybně třeba zvážit. Na druhou stranu se mi ale nejeví jako reálné, že by něco takového bylo možné. Dá se totiž očekávat, že vývoj by pokračoval někde jinde.

Tento stav nahrává společnostem, které za vývojem AI stojí. Jejich představitelé ale zároveň moc dobře vědí, že změna současné situace, kdy neexistuje regulace, je jenom otázkou času. Proto tyto firmy samy usilují o to, aby využití nástrojů AI bylo bezpečné. Z mého pohledu je teď důležitější pracovat na rozvoji opatření, které zajistí ochranu společnosti, a současně ve vývoji umělé inteligence nezůstat pozadu.

Ivan Bartoš říká

„Představitelé společností, které stojí za vývojem AI, dobře vědí, že změna situace, kdy neexistuje regulace, je jenom otázkou času.“

Česká republika si vede dobře

Česko si z hlediska kyberbezpečnosti v porovnání s ostatními demokratickými zeměmi vede poměrně dobře, na úrovni Evropské unie se řadíme mezi státy s vysokým stupněm kybernetické bezpečnosti. Co ale určitě potřebujeme zlepšit, je spolupráce mezi jednotlivými resorty a centrálními experty na kyberbezpečnost a IT, třeba Národním úřadem pro kybernetickou a informační bezpečnost. Kabinet pro digitalizaci, který na Úřadu vlády vedu, v tomto směru připravuje například přechod státních webů na jednotnou doménu. Ministerstvům jejich stránky zůstanou, ale jejich název se připojí k doméně gov.cz. Díky tomu se zajistí větší přehlednost, důvěra a zabezpečení před útoky.

Je samozřejmě třeba dělat řadu dalších konkrétních kroků. Zvláště důležité jsou osvěta a individuální vzdělávání. Pokud budou mít lidé povědomí o tom, jak se chránit před riziky a jak rozpoznat podezřelé aktivity, můžeme tím mnoha kybernetickým útokům předejít. Individuální vzdělávání by mělo být zaměřeno na základní zásady kybernetické bezpečnosti a výcvik by měl být dostupný všem uživatelům internetu.

Velmi důležitá jsou také systémová opatření na úrovni států, které by měly vytvořit zákony a politiky, jež budou občany a firmy před kybernetickým nebezpečím chránit. To může zahrnovat pravidelné kontroly zabezpečení firem, povinné šifrování dat a vynucování zodpovědnosti za kybernetické útoky. Státy by také měly podporovat výzkum a vývoj v oblasti kybernetické bezpečnosti, aby se mohly novým hrozbám lépe přizpůsobit.

Autorem textu je Ivan Bartoš, ministr pro místní rozvoj ČR a místopředseda vlády

V 17 letech odjel studovat do USA, kde také úspěšně odmaturoval. Později získal doktorát v oboru informační studia a knihovnictví na Filozofické fakultě Univerzity Karlovy a také absolvoval jeden semestr na Fakultě počítačových věd na University of New Orleans. Profesně působil v několika českých a nadnárodních společnostech v oboru informačních technologií. Je dlouholetým předsedou České pirátské strany.

Bankovní spolupráce

KB již sdílí bankomaty s Air Bank, Moneta Money Bank a UniCredit Bank

Zvýšit dostupnost hotovostních služeb pro klienty a současně akcelerovat aktivity v zájmu udržitelného rozvoje. To je cílem společného projektu sdílení bankomatů zmíněných finančních ústavů. Už vloni Komerční banka v tomto smyslu zahájila spolupráci s Moneta Money Bank a letos se připojily i další dvě banky. Společně tak nabízejí už více než 2 000 sdílených bankomatů.

Výběr hotovosti je jednou ze základních bankovních služeb, proto se všechny čtyři zúčastněné banky dohodly na tom, že svým klientům umožní výběr hotovosti ze všech partnerských bankomatů za stejných cenových podmínek jako ve vlastní bankomatové síti. A také na tom, že stojí-li vedle sebe

Export Journal komentuje

Banky dnes společně nabízejí už více než 2 000 sdílených bankomatů. Lze díky tomu optimalizovat náklady a také pozitivně ovlivnit životní prostředí.

na jednom místě dva sdílené bankomaty, přesunou jeden z nich tam, kde předtím nebyl žádný. Došlo k tomu už v desítkách případů.

Jak už bylo zmíněno, důvodem pro sdílení bankomatů není jenom zvýšení dostupnosti a komfortu klientů, ale také podpora udržitelnosti. Lze totiž díky tomu rovněž optimalizovat náklady, jako je elektřina, údržba, doplňování peněz a řada dalších, což samozřejmě pozitivně ovlivňuje přírodu a životní prostředí.

Komerční banka získala za inovativní přístup v oblasti sdílení bankomatových sítí prestižní ocenění Bankovní inovátor 2022, které v rámci soutěže Visa Nejlepší banka udělují Hospodářské noviny. Podrobnější informace o projektu, mimo jiné i o tom, na kterých místech České republiky je možné sdílené bankomaty využít, najdete na internetové stránce www.sdilenybankomat.cz.

KB zastavila odchozí platby do Ruska a Běloruska

Komerční banka už od začátku letošního března neprovádí platby do Ruska a Běloruska, a to v žádné měně. K tomuto rozhodnutí, které jde nad rámec zákonných sankcí, dospěla s ohledem na události související s válkou na Ukrajině, způsobené ruskou agresí se zapojením Běloruska. Platby do zmíněných zemí jsou vnímány jako mimořádné bezpečnostní riziko. Platí, že tím není dotčeno zpracování plateb z obou zemí, zároveň však nelze vyloučit jejich nepřijetí či delší dobu zpracování, a to z důvodu detailního prověřování takových plateb.

Digitalizace

V Komerční bance vyřídíte spoustu požadavků online

Komerční banka si podle svých představitelů dobře uvědomuje, že málokterý podnikatel či manažer má v současném rychlém světě času nazbyt. Proto se banka intenzivně zaměřuje na to, aby její klienti vyřídili maximum svých potřeb a požadavků online, popř. prostřednictvím zákaznické linky.

Takových služeb v KB rychle přibývá. Co všechno už dnes mohou podnikatelé řešit online?

Spravovat své platby
Tedy např. zadávat běžné platby či platby s FX kurzem, kontrolovat je a také autorizovat či zadávat a spravovat trvalé příkazy.

Spravovat platební karty
Mohou kartu zamknout i odemknout, změnit si PIN a limity, požádat o nový design karty nebo podat reklamaci transakce uskutečněné kartou. Dále si mohou aktivovat Apple Pay, Google Pay, FitBit Pay nebo Garmin Pay.

Provést základní nastavení účtu
To mimo jiné znamená přidání přístupu do účtu zmocněné osobě a nastavení limitů pro ni, nastavení Mobilní Banky Business či dočasné navýšení limitu pro platby přes internetové a mobilní bankovnictví ad.

Sjednat si nové produkty
To je např. pojištění karet Profi Merlin, čerpání podnikatelských úvěrů nebo třeba žádost o vyhotovení zprávy pro účely auditu.

Získat důležité e-dokumenty
Mimo jiné elektronické výpisy, smlouvy k produktům nebo přístup k archivu vybraných smluvních dokumentů.

Založit i aktivovat aplikaci KB Klíč
KB Klíč je tedy možné online sjednat, nastavit u něho přihlašování a podepisování, popř. i obnovit přístup.

Jaké jsou výhody elektronické komunikace s Komerční bankou?

Online správa oprávnění k dokumentům

Flexibilita
možnost vícenásobného podepisování

Přehled
systém upozornění a urgencí prostřednictvím MB, MBA a e-mailu

Archiv dokumentů dostupný kdykoli a odkudkoli, bezpečný, zdarma, doživotní platnost, přerazítkování pro zajištění validity

Bezpečnost
nejvyšší úroveň zabezpečení (KB Klíč, certifikát, Trusteer Rapport)

Úspora času
bez nutnosti osobní návštěvy (ať už klienta na pobočce, nebo bankovního poradce u klienta)

Komfort
možnost řešit požadavky kdykoli a odkudkoli 24/7 (na služební cestě, v noci, ...)

Dostupnost
PC i mobilní telefon

Stačí se přihlásit do internetového bankovnictví MojeBanka Business a Mobilní banka Business. Kliknutím na link MojeBanka Business u jednotlivých požadavků se uživatel nejprve dostane na stránku přihlášení a po vyplnění přihlašovacích údajů bude přesměrován tam, kam potřebuje.

Export Journal komentuje

KB svým klientům nabízí možnost vyřídit si maximum požadavků z pohodlí domova či z firmy. Podnikatelé si takto mohou sjednat nové produkty, čerpat podnikatelský úvěr nebo získat důležité dokumenty.

Budějovický Budvar je z globálního hlediska světovým unikátem

S exportní ředitelkou Budějovického Budvaru Renatou Pánkovou o jeho úspěchu na exportních trzích za poslední víc než dekádu, o tom, jak se prodává prémiový ležák do Jihoafrické republiky či Tádžikistánu nebo jak se mění trendy v pivovarnickém sektoru.

Podle statistik to vypadá, že se covidová pandemie Budvaru na zahraničních trzích prakticky nedotkla. Za rok 2020 jste oproti předešlým obdobím dosáhli exportního rekordu a to samé platí pro rok 2021. Jak je to možné?
Budvar se v těchto letech stal českou exportní pivní značkou čísla jedna. Každá láhev, plechovka či sklenice točeného piva, na které kdekoliv na světě narazíte pod značkou Budweiser Budvar, Budějovický Budvar anebo Czechvar (z důvodu známkoprávního nesmíme na americkém kontinentě užívat označení obsahující tři písmena BUD), je vždy vyrobena na jednom místě – v Českých Budějovicích. Budvar jako národní podnik je z globálního pohledu v podstatě světovým unikátem, což nám zaručuje nezávislost a také jakousi konkurenční výhodu. Na druhou stranu nemáme tak velký kapitál a tržní sílu jako naši největší konkurenti či jiná česká piva, která patří do velkých mezinárodních pivovarnických skupin. Tím je částečně ovlivněna struktura našeho obchodu.

Co konkrétně stálo za úspěchem v období pandemie?
Jednak to, že větší podíl vyvezeného piva prodáme v off trade. To se v covidové době, kdy se spotřebitelská poptávka z důvodu uzavřeného segmentu gastronomie přesunula do obchodů, ukázalo jako výhoda. Zároveň se ale pozitivně projevila naše dlouhodobá strategie. Daří se nám totiž trvale udržovat prémiovou pozici, kdy naše pivo patří v každé zemi, kam vyvážíme, vždy mezi nejdražší ležáky. A protože lidé nemohli téměř nikam chodit, tak si alespoň doma dopřávali ty nejkvalitnější produkty, mezi které naše pivo, vařené stále tradičním způsobem, jednoznačně patří. Také jsme se jako firma dokázali rychle přizpůsobit novým způsobům práce a výzvám, které covid přinášel.

Budvar se ale může pochlubit výbornými výsledky za celou poslední dekádu, nejen za tyto dva roky.
Ano, mohu s velkým potěšením konstatovat, že jsme dokonce za posledních patnáct let až do roku 2022 v podstatě neustále rostli. V objemu i hodnotě. To byl skvělý úspěch, na který jsme si pochopitelně rádi zvykli. Běžný vývoj společnosti i ekonomiky ve světě, který byl navíc významně ovlivněn mimořádnými událostmi (jako byla pandemie covidu a následně ruská agrese proti Ukrajině) v posledních třech letech, mají vliv i na trendy v našem oboru.

Jaké například?
Pokusím se toto široké téma stručně vystihnout. Obecně lze říct, že celosvětově klesá spotřeba piva na hlavu. To postihlo i Českou republiku, byť stále držíme první místo v mezinárodním žebříčku. Klesá konzumace piva v restauracích. Světová recese, dvojciferná inflace, rostoucí náklady ve všech sférách našeho života se promítají do kupní síly spotřebitelů. Prémiové importované výrobky si dnes v některých zemích může dovolit méně lidí než dříve. Za posledních deset patnáct let vzniklo mnoho řemeslných pivovarů, které mohou díky maloobjemové řemeslné výrobě spotřebitelům nabídnout mnoho různých variant piv. Do popředí zájmu se dostává lokální výroba, ať už z ekonomických důvodů, kvůli komplikované přepravě či proto, že spotřebitelé sympatizují s místními výrobci. Lidé se dnes snaží žít mnohem zdravěji, dbají více na to, co konzumují, nebo vůbec nepijí alkohol. Prodej nealkoholického piva roste poslední roky dvojciferně. Mladí lidé jsou méně loajální k jedné značce piva, než byly generace konzumentů třeba před dvaceti lety. Téma trvalé udržitelnosti, odpadové hospodářství a ekologické zdroje energie mají také vliv na výrobu i prodej piva. I když všechny tyto trendy či vývojové změny platí obecně pro celý svět, je potřeba říct, že se liší či mohou lišit země od země či region od regionu. Ať už mluvíme o vývoji v čase či intenzitě.

Díky čemu je Budvar na exportních trzích rok od roku úspěšnější? A co všechno jste v pivovaru během svého působení změnila?
To je složitá otázka. Platí ale, že za mého působení v roli exportní ředitelky jsme toho s kolegy dokázali docela dost. Od roku 2005 jsme téměř ztrojnásobili objem vyvezeného piva. Přitom se nám dlouhodobě daří držet prémiovou cenu v prémiovém segmentu mezinárodních piv. Zvládli jsme skoro zdvojnásobit počet zemí, do kterých vyvážíme. Založili jsme tři dceřiné společnosti – v Německu, ve Velké Británii a na Slovensku –, abychom na klíčových trzích sami řídili obchod, marketing i distribuci. Rozšířili jsme budvarské portfolio na zahraničních trzích o další naše skvělé produkty, jako je tmavé pivo či nealko, otevřeli desítky tankových restaurací v Británii, na Slovensku a v Polsku, loni naši první tankovou provozovnu ve Vídni. Budvar si dnes můžete dát třeba i v plážovém baru luxusního hotelu Palace of Emirates v Abú Dhabí atd.

Vaše exportní oddělení tedy zřejmě funguje velmi dobře. V čem vidíte jeho hlavní přednosti?
Včetně kolegů v dceřiných firmách je nás dnes dohromady již téměř sto, v týmu jsou lidé několika národností. O to víc musíme klást důraz na to, abychom jako tým také správně spolupracovali. Což zároveň znamená, že každý dobře plní svoji roli a cítí se plně zodpovědný za svoji agendu. Ať jsou to individuální role, anebo mini týmy, jako třeba zákaznický servis, regionální týmy pro rozvoj našich zahraničněobchodních aktivit, globální trade marketing, administrativa anebo týmy v našich zahraničních dceřiných společnostech. Proto se snažíme starat o rozvoj všech kolegů a vytvářet při práci dobrou atmosféru. Pro mě je vždycky na prvním místě charakter lidí a pozitivní energie, chuť pracovat. Všechno ostatní se naučíte. Jednou z našich silných stránek je určitě i zdravá soutěživost, tah na branku.

Budvar dnes své pivo prodává do víc než sedmdesáti zemí světa a mezi nimi jsou z pohledu laika možná trochu netradiční trhy jako třeba Alžírsko, Kamerun, Ekvádor, Peru či Filipíny. Jak obtížné je prosadit se v těchto státech?
Platí, že čím vzdálenější, tím je exportní trh také odlišnější. Z technického hlediska je například mnohem dražší a složitější přeprava, někde platí vysoká dovozní cla, musíme splňovat různé legislativní či kvalitativní požadavky a podobně. Na obchodní vztahy mají samozřejmě vliv také kulturní rozdíly, roli hraje třeba i případná politická nestabilita nebo náboženství. Pokud do takových zemích chcete vyvážet, musíte všem těmto věcem rozumět a umět s nimi pracovat. Proto mě moc těší, že se nám v letošním roce podařilo poprvé exportovat do Jihoafrické republiky nebo třeba do Tádžikistánu.

Renata Pánková, exportní ředitelka Budějovického Budvaru

Kyberprostor v ohrožení

Jak NÚKIB hlídá kybernetické Česko

O kybernetickou bezpečnost České republiky na institucionální úrovni pečuje Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Jeho úkolem je chránit jak kyberprostor v této zemi, tak i kyberprostor každého občana naší republiky. Co všechno v této oblasti úřad dělá a jak hodnotí současný stav?

Jak jsme už zmínili v jiných článcích tohoto vydání Export Journalu, z pravidelných Zpráv o stavu kybernetické bezpečnosti vyplývá, že v posledních letech počet tzv. incidentů výrazně stoupá. Bezpečnostní komunita upozorňuje například na kybernetickou špionáž provozovanou cizími státními aktéry, pravděpodobně zejména z Číny a Ruska, nebo jimi sponzorovanými skupinami v českých sítích. Výsledkem pak může být mimo jiné kompromitace citlivých a utajovaných informací anebo ztráta obchodních tajemství, což vede k oslabení konkurenceschopnosti. Hrozí také úniky dat, útoky skrze slabá místa v dodavatelském řetězci nebo i útoky na volební proces.

Častými cíli jsou přitom univerzity, subjekty v bankovním sektoru a energetice, subjekty kritické infrastruktury, veřejný sektor a koncoví uživatelé coby brána do sítí organizací. V posledních měsících jsme také byli svědky rostoucího množství útoků na zdravotnická zařízení a citlivé zdravotní údaje. Například na začátku covidové pandemie způsobili kyberútočníci Fakultní nemocnici Brno škody ve výši 150 milionů korun.

Terč na záda

Zpráva úřadu za rok 2022 zatím nebyla zveřejněna, ale podle Lukáše Kintra, ředitele NÚKIB, platí, že útočníci neustále vyvíjejí nové techniky, zdokonalují se a snaží se své oběti zaskočit. „Základní typy útoků nicméně zůstávají stejné. I nadále nejčastěji čelíme útokům na dostupnost, tedy DDoS útokům, podvodným phishingovým kampaním, různým škodlivým kódům a pokusům o průnik," vysvětluje Lukáš Kintr.

NÚKIB ve zprávě za rok 2021 současně konstatuje, že u čtvrtiny respondentů došlo následkem útoku k narušení důvěrnosti, integrity nebo dostupnosti informací či služeb. Je to ve srovnání se zeměmi, které jsou na tom z pohledu kyberbezpečnosti nejlépe, hodně, či málo? Ředitel NÚKIB odpovídá, že státy z bezpečnostních důvodů stav své kybernetické bezpečnosti příliš do detailu nerozvádějí. „Bylo by to jako namalovat si terč na záda. Navíc metody, kterými se vyhodnocují různé parametry, jsou stát od státu odlišné. Obecně vzato má Česká republika bezpochyby prostor pro zlepšení, ale to platí pro všechny státy. Kyberbezpečnost je totiž nikdy nekončící proces."

Vše, co Česká republika potřebuje

Logicky se tedy nabízí otázka na onen prostor pro zlepšení. Vše, co aktuálně Česko potřebuje, je podle Lukáše Kintra obsaženo v novém zákonu o kybernetické bezpečnosti, který jeho úřad aktuálně připravuje. Norma je prý mj. reakcí na dynamický vývoj v bezpečnostním prostředí a její součástí je také nová bezpečnostní směrnice EU, tzv. NIS2, i mechanismus na prověřování rizikovosti dodavatelů ICT do strategicky významné infrastruktury České republiky.

Směrnice je už platná a v současnosti probíhá její implementace do právních řádů členských států. Dlužno dodat, že NÚKIB se na její přípravě také podílel. Norma ovšem podle Lukáše Kintra přináší takové množství změn, že úřad upustil od původně plánované novely a jeho specialisté sepsali zcela nový zákon o kybernetické bezpečnosti. Podle informací z médií úřad na jeho návrh letos obdržel z trhu a od státních institucí včetně ministerstev tisíc připomínek. A objevila se také kritika.

Podle ní například hrozí, že NÚKIB ze sebe zákonem vytvoří „superúřad" s možností určovat si rozsah regulace, zasahovat do působnosti ministerstva zahraničních věcí, vlády apod. „Nic takového jako ‚superúřad' z NÚKIB nebude. Budeme jednat z pověření vlády, dle zákonem stanovených kompetencí a rozhodovat na základě informací a dat od našich spojenců a partnerů. Finální konzultace pak budou probíhat nejen na straně státu, ale také s dotčenými subjekty," dodal ředitel Kintr.

Běh na dlouhou trať

Kybernetická bezpečnost je běh na dlouhou trať, říká ředitel NÚKIB Lukáš Kintr s tím, že měřit okamžité výsledky je obtížné. Všichni bychom se však podle něj měli věnovat osvětě, a to se týká všech věkových kategorií. „Proto na našem webu osveta.nukib.cz najdete kurzy, které pomohou v oblasti kyberbezpečnosti každému z nás. Proto se podílíme na aktivitách, jako jsou Kyberpohádky nebo kampaň České bankovní asociace #nePINdej, a proto sami děláme opravdu velké množství vzdělávacích akcí, kampaní, konferencí a webinářů pro rozmanité cílové skupiny. Je to mravenčí práce, která nejde jen za námi. Osobně mi chybí systémové řešení této oblasti ze státní, vzdělávací úrovně," uzavírá Lukáš Kintr.

Obrovské rozdíly mezi firmami

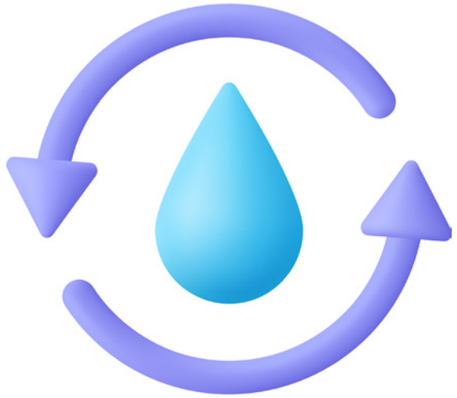
Pokud jde o situaci v soukromém sektoru, Lukáš Kintr vysvětluje, že úřad má ze zákona podrobné informace o přibližně čtyřech stovkách subjektů, které jsou nejdůležitější pro fungování státu. „Z dat, která máme o subjektech mimo regulaci zákona o kybernetické bezpečnosti, je však zřejmé, že mezi jednotlivými firmami jsou obrovské rozdíly. Jednak jsou společnosti, které si nebezpečí plně uvědomují, což se jim také jednoznačně vyplatí. Druhé skupině pak přeji, aby se jich netýkal žádný kybernetický incident, protože následné škody by pro ně mohly být likvidační," zdůrazňuje ředitel NÚKIB.

Rozsah činností a aktivit, kterými se úřad snaží vylepšovat kybernetickou bezpečnost České republiky, je opravdu široký. Kromě regulace a kontroly, což vedle zmíněné přípravy zákona o kybernetické bezpečnosti zahrnuje také třeba posuzování nabídek cloud computingu podle zákona o informačních systémech veřejné správy, je to několik dalších oblastí. Především vzdělávání, v jehož rámci NÚKIB připravuje e-learningové kurzy kyberbezpečnosti či různé konference, semináře a workshopy (více viz box). Je to také organizace a příprava kybernetických cvičení, která umožňují simulovat rozličné typy krizových situací. NÚKIB je současně hlavním národním kontaktním centrem v oblasti výzkumu a vývoje v kybernetické bezpečnosti a ochrany utajovaných informací. A v neposlední řadě připravuje Národní strategii kybernetické bezpečnosti České republiky včetně akčního plánu.

Lukáš Kintr,
ředitel Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB)

Hospodaření s vodou je pro řadu firem klíčové

Opravdu je to tak. A to nejen kvůli stále rostoucí ceně vody, ale v řadě případů také kvůli její omezené dostupnosti. Spotřeba vody je často vyšší než množství produkované výroby, třeba pivovary spotřebují na sto litrů piva kolem 2 500 litrů vody ap. Když se tedy sečtou veškeré náklady, včetně čištění odpadních vod a dalších, náklady za vodu pro podniky jsou opravdu vysoké. Proto se firmy snaží ji co nejvíce recyklovat, což se mnohdy daří, byť jsou zde určité omezující podmínky.

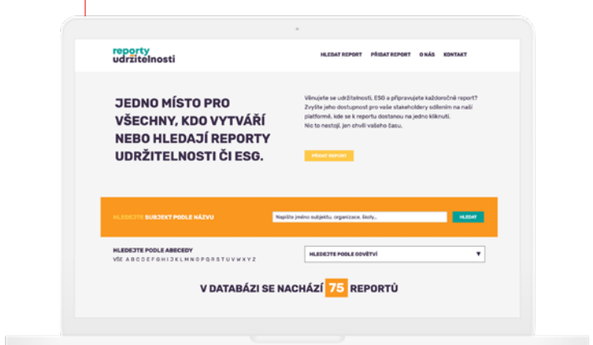


Zájem o vodní audit roste

Při hospodaření s vodou může pomoci vodní audit. Poskytuje ho poradenská společnost Enviros, která je součástí Skupiny KB. Jiří Klicpera z Envirosu vysvětluje, že využívání vodního auditu se teprve rozbíhá, ale některé výsledky už jsou k dispozici. „Zkušení auditoři dobře vědí, kam sáhnout pro úspory a kde najít nepřesnosti nebo podněty ke zlepšení. Proto nabízíme podnikům služby zkušených auditorů, aby jim pomohli co nejvíce snížit nároky na vstupní pitnou vodu," říká Jiří Klicpera. K řadě činností v podnicích totiž pitná voda není potřeba, stačí voda srážková nebo recyklovaná, což platí zejména pro nejrůznější chladicí okruhy nebo pro stavebnictví. Podle Jiřího Klicpery je třeba dbát na to, aby náklady vynaložené na úspory vody nevedly k extrémnímu zvýšení ceny výrobku.

Jiří Klicpera firmám doporučuje, aby se dobrovolně vrátily k dříve povinné praxi, kdy existovala funkce odborných podnikových vodohospodářů. „Ti se scházeli na odborných konferencích, seminářích či kurzech, sdělovali si své zkušenosti a konzultovali problémy, dokonce často zcela zdarma. Tahle praxe by mohla řadě podniků dost pomoci," myslí si Jiří Klicpera. Také by podle něj pomohlo zaměřit se na snižování ztrát vody v rozvodné síti podniků. Voda, která kdekoli unikne do země, se už do okruhu pochopitelně nevrátí. Což je (nejen) vzhledem k tomu, že nebyla levná, zbytečný luxus.

Všechny reporty udržitelnosti na jednom místě



Portál reportyudrzitelnosti.cz slouží ke sdílení reportů z oblasti udržitelnosti a ESG napříč firemním sektorem. Myšlenka je jednoduchá: Společnost, která o to stojí, může jednoduše a zdarma svůj report na web nahrát. Tím podle představitelů poradenské firmy Fair Venture, která za webem stojí, zvyšuje pro stakeholdery dostupnost informací o svých aktivitách v oblasti udržitelnosti a ESG. Reporty lze na portálu hledat podle názvu organizace anebo také podle odvětví. V době vzniku tohoto článku, tedy zhruba v polovině června, bylo na portálu dostupných sedmdesát jedna zpráv. Mezi jinými od společností ČEZ, Vodafone, Kofola, Kaufland, Plzeňský Prazdroj či Biopekárna Zemanka a samozřejmě také od Komerční banky.

www.reportyudrzitelnosti.cz

Firemní centra KB – nepostradatelný partner pro podnikání

V každé ze svých dvaceti páteřních poboček nabízí Komerční banka kompletní poradenství živnostníkům a malým podnikům v rámci sítě Firemních center. A to v rozsahu, který byl po dlouhou dobu vyhrazen pouze velkým firmám.

Podnikatelé a živnostníci mohou v rámci Firemních center díky přístupu k nabídce produktů i dalších členů finanční skupiny KB získat odborné poradenství nebo vyřešit prakticky veškeré záležitosti, které se týkají jejich podnikání. Ať už jde o úvěry, financování provozu firmy, nákup materiálu nebo zásob, leasing či financování provozu vozidel a dopravní techniky, také třeba fakturace, pojištění, využívání fondů EU anebo celou řadu dalších důležitých oblastí.

Prostory center, která jsou k dispozici v rámci poboček ve velkých městech po celé České republice, jsou pro tyto účely speciálně upravené. Umožňují tedy mimo jiné představit zájemcům řadu užitečných aplikací, jako je mobilní bankovnictví pro firemní klienty nebo internetová platforma pro ošetření měnových rizik. V rámci služeb Firemních center se mohou majitelé a firemní management služeb spolehnout i na to, že bankovní specialisté zvládnou pokrýt také jejich individuální potřeby, a to včetně nabídky produktů pro zaměstnance.

Pracovníci center ovšem poskytují odborné poradenství a individuální služby nejen klientům z velkých měst, ale i podnikajícím osobám z menších lokalit. Původní pobočky v těchto místech jsou přitom klientům stále k dispozici. Mohou tam tedy i nadále využívat služeb každodenního bankovnictví a provádět hotovostní operace tak, jak jsou zvyklí. Pokud potřebují složitější služby či individuální řešení, jednoduše si domluví schůzku s bankovním poradcem. Dalším benefitem je možnost komunikovat v případě zájmu s poradcem, popř. dalšími specialisty banky i na dálku. Videorozhovor probíhá v prostorách Firemního centra KB, na domácí pobočce klienta nebo v místě, které klient preferuje, například v jeho provozovně či v sídle společnosti.

Produkty pro snadnější podnikání

- **Digitální dílna** – tvorba webu na míru
- **iÚčto** – účetnictví včetně párování příchozích plateb s fakturami pro firmy i živnostníky
- **Fakturoid** – rychlé online vystavení faktur s hlídáním splatnosti
- **Paymium** – platební tlačítko pro firemní e-shop
- **Firma pro vás** – založení firmy zdarma, klient zaplatí jen zákonné poplatky
- K účtu lze získat **platební terminál / PayPhone** na 12 měsíců zdarma v rámci akce Česko platí kartou
- Možné je získat **kreditní kartu pro podnikatele** a dostávat 1 % z plateb zpět na podnikatelský účet (cashback)
- K podnikatelskému účtu lze získat **kontokorent** s limitem až 3 000 000 Kč

Ekonomika

Česká ekonomika v zajetí cen energií

Česká republika je jednou z nejvíce zranitelných zemí, pokud jde o dostupnost energií, a to nejenom dostupnost fyzickou, tedy zda energie vůbec budou, ale i tu finanční, to znamená, za kolik budou tyto zdroje dostupné.

I s ohledem na charakter tuzemského hospodářství jakožto průmyslové, a tedy energeticky náročné země je otázka energetické dostupnosti zásadní. Z pohledu vyprodukovaného hrubého domácího produktu patří Česko mezi ty evropské země, jejichž energetická náročnost je jedna z nejvyšších. A bohužel to o moc lépe nevyznívá ani na straně tuzemských domácností. Podíl výdajů za energie na celkových výdajích českých domácností je opět jeden z nejvyšších v Evropě. Není tedy divu, že ceny energií jsou alfou a omegou nejenom spotřebitelské a podnikatelské důvěry, ale potažmo celé ekonomiky.

Poslední více než rok byl ve znamení opravdových veletočů na cenách energetických komodit – plynu, elektrické energie i ropy, potažmo pohonných hmot. Napadení Ukrajiny ze strany Ruska loni na jaře vyvolalo dramatický nárůst cen. Ten byl důsledkem zejména výrazné energetické závislosti na Rusku. Sankce uvalené na Rusko a snaha se co nejrychleji této závislosti zbavit vedly k nárůstu cen, zejména plynu a elektřiny, na historicky nejvyšší úrovně. Ty kulminovaly během léta, kdy se ukázalo, že plynové zásobníky v Evropě se před nadcházející zimou relativně rychle plní. Až nepředstavitelná akceschopnost Evropské unie stála za opravdu razantní strukturální změnou v případě dovozu plynu, a to ve zkapalněné formě (zejména LNG). Budování nové infrastruktury v kombinaci s mírnou zimou způsobilo, že se ceny energetických komodit otočily a v průběhu prvních měsíců letošního roku postupně klesly na úroveň před válkou na Ukrajině.

Jan Vejmělek, hlavní ekonom Komerční banky

Stagflační syndrom

Loňský nárůst cen vedl ke stagflačnímu syndromu. Významně přispěl k celosvětovému vzestupu inflace na straně jedné a útlumu reálného hospodářského růstu na straně druhé. Globálně inflace kulminovala přibližně v závěru loňského léta, což primárně souviselo s již zmíněnými cenami energetických komodit. Významnou složkou na straně inflace byla ale i ta poptávková, což platilo například pro Spojené státy, ale třeba i pro Česko. Zde se jednalo zejména o důsledek expanzivní měnové i fiskální politiky z období koronavirové pandemie. Z hlediska dopadu do reálné ekonomiky se vysoké ceny energetických vstupů promítly do výrazného ochlazení růstu prakticky po celém světě v druhé polovině loňského roku a během prvních měsíců toho letošního.

Vývoj tuzemské ekonomiky do značné míry kopíroval zmíněný globální vývoj. Stagflační rysy byly patrné i v Česku. Meziroční míra inflace v průběhu roku 2022 zrychlovala a kulminovala v září na 18,0 %. Dalšímu nárůstu zabránilo dočasné zavedení vládního úsporného energetického tarifu na závěrečné tři měsíce loňského roku. Lednová meziroční inflace ještě činila 17,5 % a od té doby každý měsíc klesá.

Ekonomika mírně roste, inflace klesá

Z pohledu reálné ekonomiky prošlo české hospodářství v druhé polovině loňského roku technickou recesí. To znamená, že byl dvě čtvrtletí po sobě vykázán mezičtvrtletní pokles reálného hrubého domácího produktu. Během třetího čtvrtletí HDP klesl o 0,3 % oproti předchozímu čtvrtletí, v průběhu závěrečného kvartálu loňského roku to bylo o 0,4 %. S nástupem roku 2023 ale hospodářský pokles skončil. Proto recesi chápeme pouze v technickém slova smyslu, nijak totiž nepomohla v boji s vysokou inflací ani s uvolněním na napjatém trhu práce. A z tohoto důvodu spíše než o stagflaci hovoříme o stagflačních symptomech. Pro typickou stagflaci je totiž charakteristické výrazné zhoršení na trhu práce v podobě nárůstu nezaměstnanosti. Nic takového v našem případě nenastalo.

Již první měsíce tohoto roku ukázaly, že loňský stagflační obrázek je minulostí, stagflační symptomy jsou na ústupu. Zatímco růstové vyhlídky pro letošní rok jsme v dubnové prognóze revidovali mírně směrem k vyšším hodnotám, u inflace tomu bylo naopak. To ale nic nemění na tom, že hospodářský růst bude letos utlumený. Aktuální prognóza počítá s dynamikou pouze 0,6 %. To by znamenalo, že se Česko jako jedna z posledních evropských zemí vrátí na předpandemickou úroveň až v druhé polovině letošního roku. Průměrná inflace pak bude i letos v průměru dvouciferná, když ji čekáme na 11,8 %. Dosavadní vývoj klíčových ekonomických agregátů v letošním roce ukazuje pro naši růstovou prognózu riziko nepatrně nižší celoroční dynamiky, u inflace je šance na celkově nižší cenovou dynamiku o něco výraznější.

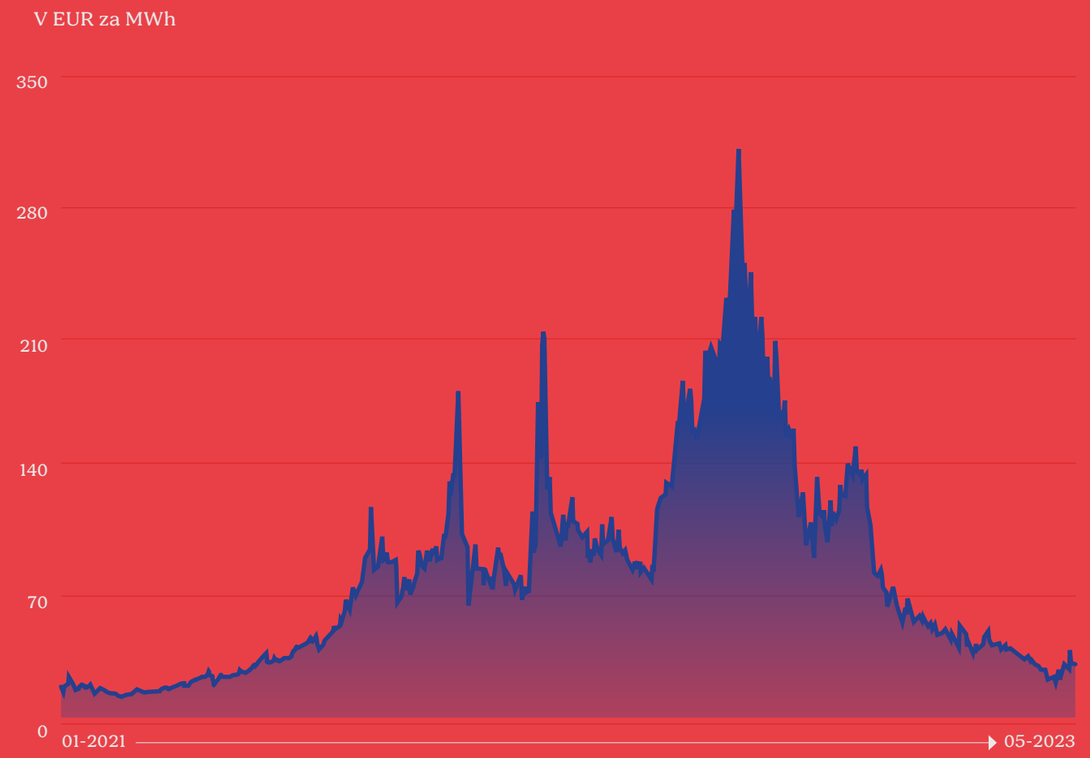
Národní účty za první čtvrtletí letošního roku ukázaly, že v mezičtvrtletním vyjádření česká ekonomika stagnovala, zatímco my jsme očekávali růst, byť nevýrazný, o 0,2 %. Původní rychlý odhad ČSÚ přitom ukazoval na nepatrné zlepšení o 0,1 %. Oproti předpandemickému poslednímu čtvrtletí roku 2019 byl HDP v letošním prvním čtvrtletí stále nižší o 1 %.

Dařilo se exportérům

Na relativně slabý výkon ekonomiky nadále působí (hlavně v souvislosti s vysokou inflací a poklesem reálných disponibilních důchodů) klesající spotřeba domácností. Tempo jejího mezičtvrtletního poklesu se zmírnilo z −2,8 % v závěrečném čtvrtletí loňského roku na stále výrazných −1,2 % v prvním kvartále roku letošního. Výdaje domácností se tak v reálném vyjádření snižovaly již šest čtvrtletí v řadě a oproti předpandemickému období byly nižší o 9,2 %. Důvěra domácností měřená spotřebitelským sentimentem sice zaznamenala na začátku letošního roku zlepšení, reálné mzdy ale zůstaly meziročně hluboko v záporném teritoriu (oproti prvnímu čtvrtletí roku 2022 mzdy reálně klesly o 6,7 %). Zhoršení kupní síly domácností způsobené vysokou inflací tak podle všeho zůstává hlavním důvodem klesající spotřebitelské poptávky. Přetrvávající slabost celkové tuzemské poptávky pak potvrdily i klesající fixní investice. Jejich objem byl v letošním prvním čtvrtletí mezičtvrtletně nižší o 1,8 % po předchozím poklesu o 1,1 %.

Pokles spotřeby domácností v prvních měsících letošního roku vyvažoval výrazně vyšší čistý vývoz. Jeho příspěvek k mezičtvrtletní dynamice HDP činil silných 3,3 procentního bodu. Jedná se o druhý nejvyšší údaj časové řady dostupné od roku 1996, když tento příspěvek byl vyšší jen ve třetím čtvrtletí roku 2020, tedy po odeznění první vlny covidové pandemie. Na silných číslech českého exportu se podílelo oživení průmyslu související se zmírněním problémů v dodavatelských řetězcích. Výrobky z předchozích měsíců, které zůstaly rozpracované kvůli chybějícím součástkám, tak mohly být dokončeny a vyskladněny. To dokládá i výrazný pokles stavu zásob, který částečně kompenzoval vyšší příspěvek

Plyn 1YR forward



čistého vývozu. Na vyšší čistý vývoz působila i výše zmíněná slabá domácí poptávka. Zatímco tak objem vývozu během letošního prvního kvartálu mezičtvrtletně vzrostl o 2,5 %, objem dovozu se snížil o 1,3 %.

Klíčem budou opatření na podporu ekonomiky

Spotřeba vlády pokračovala v rychlém růstu v důsledku expanzivního charakteru fiskální politiky, ten byl viditelný i ve vývoji hrubé přidané hodnoty. Mezičtvrtletně byla spotřeba vlády v prvním čtvrtletí vyšší o 1,9 %, a to po již výrazném růstu o 3,8 % v závěrečném kvartále loňského roku. Hlavní vliv zde pravděpodobně měla opatření související s drahými energiemi, od začátku letošního roku pak zejména zavedení cenových stropů. Zvýšení dotací na produkty z tohoto titulu vysvětluje silný mezičtvrtletní nárůst hrubé přidané hodnoty o 0,8 %, který tak kontrastuje s pouze stagnujícím HDP.

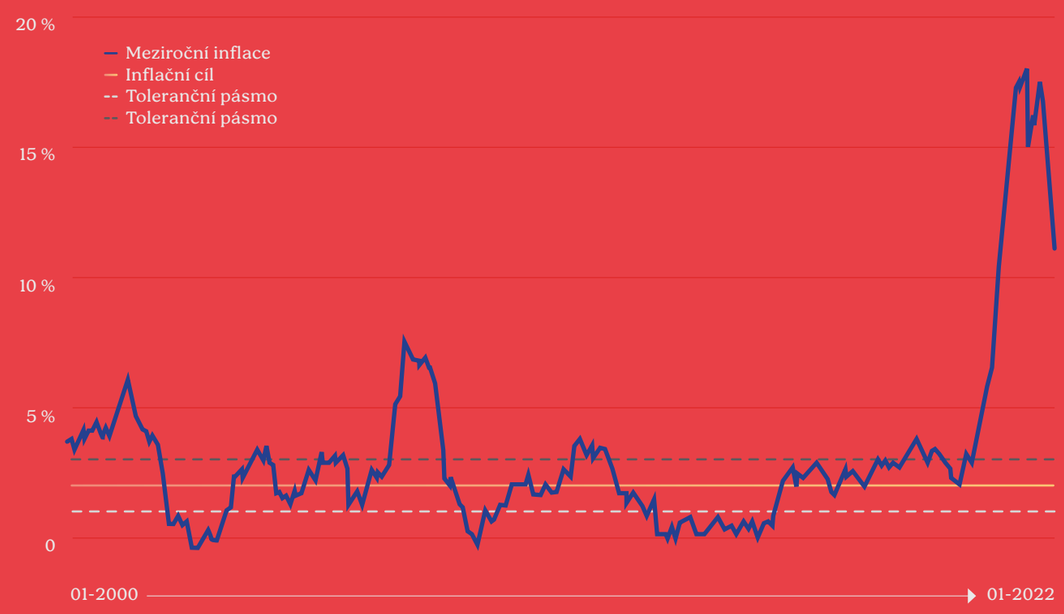
Pokud jde o současnou inflační dynamiku, zejména díky opačnému působení cen energetických komodit míří směrem dolů. Vzhledem k efektu statistické základny, kdy se srovnáváme s loňským rokem, kdy ceny energií dramaticky rostly, meziroční dynamika spotřebitelských cen rychle padá. Již červnová meziroční inflace může atakovat jednocifernou hodnotu. Pod 10 % se inflace s velkou pravděpodobností dostane s počátkem druhého pololetí a kolem 9 % se bude držet po zbytek letošního roku. Kvůli poklesu regulovaných cen pak předpokládáme, že v průběhu prvního čtvrtletí příštího roku bude inflace na cíli. Ale pozor, ne její jádrová složka! Ta zůstane i po celý rok 2024 poměrně výrazně nad dvouprocentním inflačním cílem.

Export Journal komentuje

„Pokud jde o současnou inflační dynamiku, zejména díky opačnému působení cen energetických komodit, míří směrem dolů.“

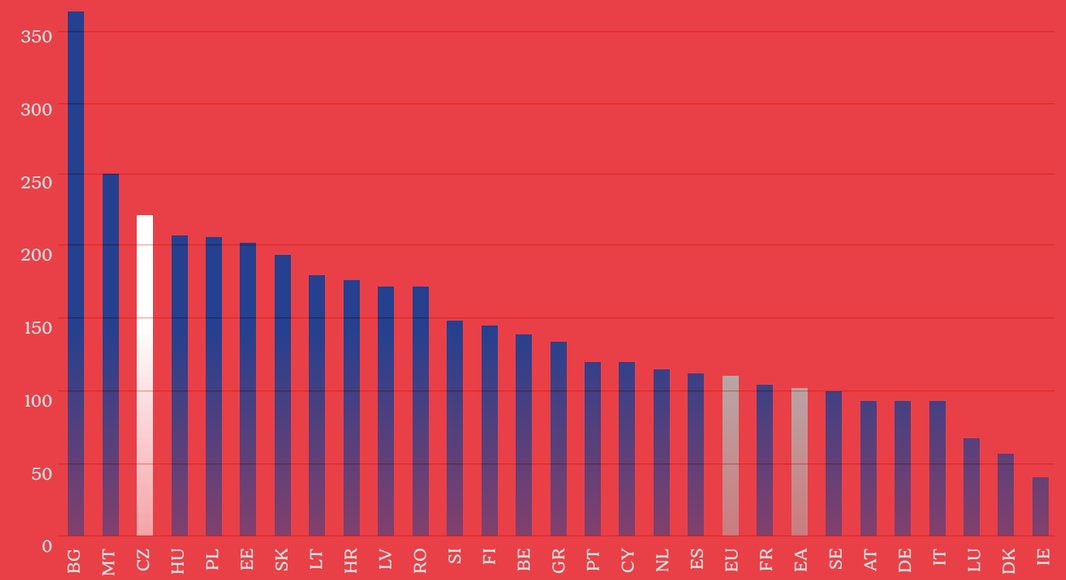
S výhledy ale ještě zamává fiskální balíček, který v průběhu května představila česká vláda. Ten však musí projít celým legislativním procesem a je otázkou, jak budou na jeho konci parametry výsledné fiskální restrikce vypadat. Každopádně se bude jednat o restrikci, nyní je otázkou pouze její kvantifikace. Výsledkem tak bude zřejmě o něco nižší inflace v příštím roce i o něco slabší hospodářský růst. Klíčové ale bude, zda se podaří prosadit taková opatření, která střednědobě a dlouhodobě naopak povedou k posílení potenciálu české ekonomiky.

Inflace vystřelila výrazně nad cíl centrální banky. To nejhorší je už za námi



Energetická náročnost produkce reálného HDP (2020)

V kg ropného ekvivalentu na 1 000 EUR



Zdroj: Eurostat

Právo a byznys

Udělali jste všechno pro zabezpečení citlivých firemních dat?

Předcházet rizikům z online světa je důležité, a to nejen co nejlepším zajištěním důležitých dat a technologických zařízení nebo školením zaměstnanců. Dostatečná úroveň kybernetické odolnosti začíná už „na papíře“, tedy přípravou důležitých interních směrnic nebo třeba ošetřením případných hrozeb ve smlouvách.

Týká se to ve větší míře exportérů, protože jim vzhledem ke komunikaci se subjekty z mnoha různých jurisdikcí hrozí větší riziko kybernetických útoků než firmám, které podnikají výhradně na domácím trhu. To ale rozhodně neznamená, že podniky, které za hranicemi nepůsobí, by se tímto problémem zabývat neměly. V článku se pokusíme nastínit alespoň některé ze zásadních aspektů, na něž by vedení firem určitě nemělo zapomínat.

Hledá se ideový otec pro kyberbezpečnost

Absolutním základem a současně možná i úplně nejdůležitějším krokem je podle advokáta Tomáše Ščerby nalezení někoho, kdo bude ve firmě působit v roli určitého ideového nositele myšlenky, že problematikou kyberbezpečnosti je třeba se vážně a poctivě zabývat. „Jestliže budou představitelé společnosti tuto věc vnímat tak, že je to zase jen něco zbytného, do čeho jsou – vzhledem ke zpřísňování příslušné legislativy – nuceni, a nikoli jako nesmírně důležitou agendu pro ochranu majetku, lidí, dobrého jména firmy a vlastně všeho, co vytváří, pak je to špatně,“ myslí si Tomáš Ščerba, který se na problematiku specializuje.

Pokud přejdeme ke konkrétním krokům, pak je třeba zabývat se především zabezpečením přenosu dat. Představitelé firem či příslušných úseků by si předně měli svá data rozdělit. Například na tzv. obchodně citlivá data, data podléhající obchodnímu tajemství, utajované informace, informace obsahující osobní údaje a pak také bezpříznakové informace. Následně je důležité věnovat pozornost tomu, jak mají firmy zabezpečený přenos výše zmíněných dat nejen v rámci organizace, ale především mimo ni. Což se týká zejména obchodních smluv, faktur, platebních informací atd., a to zejména při komunikaci se subjekty mimo Českou republiku nebo Evropskou unii.

Tomáš Ščerba doporučuje vytvoření příslušné interní řídicí dokumentace, součástí které budou mj. pravidla pro šifrování a další ochranné protokoly. Ty by měly zamezit úniku především pro korporaci citlivých obchodních informací. Jak takovou dokumentaci vytvořit? V první řadě je nutné vědět, jaká data vlastně firma potřebuje chránit. Musí tedy zjistit, jakými daty přesně disponuje, a ta pak podle vytvořené metodiky pečlivě klasifikovat.

Pozor na cloudy. Zvlášť ty americké

Pokud společnost pro uchovávání svých dat využívá zahraniční cloudové služby, svou informační bázi by si také měla zabezpečit. Především pro případ kyberútoku, tak aby neztratila přístup k datům, a tím pádem nebyla například vydíratelná (více se problematikou zabýváme v hlavním tématu vydání). To by mělo být zajištěné ideálně smluvně. Za tím účelem by vedení firmy mělo pověřit konkrétního člena týmu vypracováním návrhu příslušného dokumentu. A to podle standardu ISO 27¦000 pro normy z oblasti bezpečnostních informací, protože návrh bude obsahovat údaje o zaměstnancích, dále obchodní data, jako jsou plány, závazky, CRM dokumentace o zákaznících atd.

Tato data by pak měla být přiřazena k jednotlivým úrovním například na škále jedna až pět a u těch by se pak měla stanovit pravidla, kdo k nim má přístup apod. Poté by například zápisem z jednání představenstva, popř. jiným aktem, měla vzniknout dokumentace s tzv. pyramidální strukturou, která rozvádí stanovená pravidla do celé organizace.

Firmy, které využívají cloudové služby poskytovatelů americké provenience, by podle Tomáše Ščerby měly být opatrné dvojnásobně. Teoreticky se totiž může stát, že budou muset svá důležitá data poskytnout třeba i vládě Spojených států a jednotlivým bezpečnostním složkám. V krajním případě pak nelze vyloučit ani takový scénář, že se tyto informace mohou dostat i k jejich americké konkurenci. Zpřístupnění uložených či zpracovávaných dat americkým orgánům a bezpečnostním složkám totiž umožňuje tzv. American Cloud Act.

Jak se proti tomu bránit? „Pravděpodobně nejméně nákladnou možností je důsledně trvat na tom, aby američtí poskytovatelé cloudových služeb fyzicky uchovávali data na serverech, které jsou lokalizované v Evropské unii. To firmě umožní získat čas pro realizaci nutných kroků k efektivnímu získání dat,“ vysvětluje Tomáš Ščerba. „Data by zároveň měla být exportéry pravidelně šifrována, což znamená, že nepůjdou jednoduše dešifrovat bez další součinnosti. Provider je tedy sice poskytne, ale nebudou pro třetí stranu čitelná.“ Další možností je podle advokáta využívat služeb evropských poskytovatelů, například německých nebo francouzských, i když ty možná pro konkrétní potřeby exportérů nemusí být zcela vyhovující či cenově konkurenční.

Směrnice NIS2 může pomoct všem firmám

Samozřejmě je třeba zaměřit pozornost také na technické zabezpečení firemních zařízení a počítačových sítí. Integrální součástí této ochrany musí být pravidelné školení kybernetické bezpečnosti pro všechny role v organizaci, a to pochopitelně na různých úrovních detailu a obsahu. Vhodné je zvážit investice do již zmíněné certifikace podle ISO standardu 27 000.

Zvláštní zájem by mělo vedení firem věnovat nové právní úpravě evropské směrnice NIS2, která předepisuje řadu pravidel z této oblasti. I když se norma vztahuje na regulované subjekty, což jsou kromě firem patřících do tzv. kritické infrastruktury také všechny střední a velké podniky s významnějšími obraty a rovněž státní správa, podle Tomáše Ščerby je legislativa dobrým vodítkem i pro ostatní firmy. Podle něj jim ukazuje, jak se na regulaci připravit, jak obecně k ochraně aktiv a citlivých informací přistupovat, a to nejen v zájmu firem samotných, ale i celého ekosystému. „V posledních letech je naprosto zřejmá tendence zahrnovat mezi regulované subjekty stále širší a širší okruh firem a tenhle trend bude zcela logicky pokračovat,“ myslí si advokát. A dodává, že regulace můžou na firmy dopadnout i nepřímo. Například pokud budou součástí dodavatelského řetězce, v jehož rámci regulované subjekty působí.

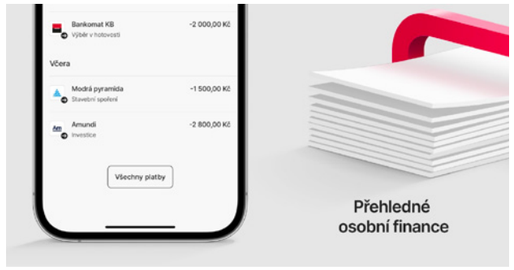
Export Journal komentuje

Problematikou kyberbezpečnosti je třeba se vážně a poctivě zabývat a nebrat ji jako něco, do čeho firmy někdo nutí. Naopak, je to nesmírně důležitá agenda pro ochranu majetku, lidí, dobrého jména firmy a vlastně všeho, co vytváří.

Tomáš Ščerba

Partner ve společnosti DLA Piper, specialista na oblast kybernetické bezpečnosti, umělé inteligence, GDPR, archivace dat či elektronického uzavírání smluv. Během své praxe se dále podílel na řadě rozsáhlých projektů v oblasti fúzí a akvizic, restrukturalizací, korporátního financování a energetiky. Mimo jiné také pravidelně přednáší na téma práva informačních a komunikačních technologií studentům českých i zahraničních právnických vysokých škol a publikuje v řadě odborných časopisů.

Komerčka představuje Novou digitální banku a mluví o revoluci



„Systém, díky kterému jsme dokázali neuvěřitelné věci, nás už teď spíše držel zpátky. A tak jsme ho rozebrali na součástky, až z něj nezbylo nic. Díváme se totiž stále dopředu, i tam, kam se nikdo jiný neodváží. Do budoucnosti bankovnictví." Těmito slovy představuje Komerční banka v rámci svého promo videa revoluční projekt, na kterém pracovala několik posledních let. Jde o Novou digitální banku, která podle představitelů banky přináší revoluční změnu, změnu banky jako takové, nejen služeb či produktů.

Co to konkrétně znamená? Hlavními charakteristikami Nové digitální banky jsou pojmy jako klient v centru dění, nejmodernější technologické nástroje či chytré produkty a služby vytvořené ve spolupráci s klienty. Tato nová éra podle KB znamená, že všechny služby jsou snadno a rychle dostupné, ať už klienti používají libovolný digitální kanál nebo pobočku. Produkty pak jsou v digitálních kanálech k dispozici na několik málo kliknutí. Služby, prodej a podpora fungují kompletně digitálně, není tedy nutné navštěvovat pobočky. Cílem také je, aby práce s bankou přinášela klientům zážitek, a to ve smyslu maximálního naplňování jejich potřeb, úspory času či skutečného obohacování jejich života.

Na co konkrétně se klienti banky mohou těšit? Například už nebudou potřebovat dvě aplikace, bude jim stačit KB+, která obsahuje KB Klíč. Díky multiměnovému účtu budou moci v reálném čase provádět konverze do měn podle kurzovního lístku a danými měnami platit a bude jim k tomu stačit jedno číslo účtu a stejná karta. Spořicí účet si klienti budou moci založit online a v jeho rámci dostanou k využití až deset spořicích obálek. Do nich si mohou odkládat peníze, na co potřebují, například obálka Železná rezerva jim pomůže s tvorbou finanční rezervy pro nečekané situace atd.

Roste obliba online tržišť

Asi jste již zaznamenali stále rostoucí oblibu a rezonování slova marketplace. Marketplace je online tržiště, kde se prodávají různé výrobky od různých prodejců, mezi které mohou patřit jak velké společnosti, tak i malé podniky a jednotlivci. V České republice jsou nejznámějšími marketplace Alza, Mall, Zoot, Zalando a na trh v Česku a na Slovensku také nově vstoupil Kaufland.

Důvodem vzniku těchto marketplace je především snaha o zvýšení konkurenceschopnosti a získání většího podílu na trhu. Pro velké společnosti je to také cesta k tomu, aby mohly nabídnout širší nabídku produktů. Využívají je převážně malé e-shopy, které nemají dostatečné zdroje pro vlastní marketingovou a prodejní kampaň. Výhodou pro prodejce je, že mohou využít již existující infrastrukturu i sílu a pověst velkých společností, aby získali více zákazníků. Pro zákazníky je to výhodné, protože mohou najít všechny produkty na jednom místě a porovnat ceny a vlastnosti zboží od různých prodejců. Nicméně, s výhodami jsou spojeny i některé nevýhody. Například ne všichni prodejci na marketplace jsou známí a ověření, což může vést ke špatnému zážitku zákazníka. Některé produkty také mohou být na marketplace dražší než u samotného prodejce.

Vzhledem k rostoucímu trendu nákupů online se očekává, že počet a význam marketplace v budoucnu stále poroste. Proto je důležité, aby zákazníci i prodejci byli obezřetní a zvažovali výhody a nevýhody nákupů na těchto platformách.

Rozvinuté země v ochraně klimatu selhávají. A ty rozvojové si to už nechtějí nechat líbit

Pařížská dohoda, která byla podepsána v roce 2015, se zapsala do dějin ochrany klimatu jako historická událost. Stala se jednak první všeobecnou a právně závaznou celosvětovou dohodou v této oblasti a také vyzvala všechny světové země k aktivnímu úsilí, které by omezilo oteplování zeměkoule na úroveň 1,5 °C, a současně vůbec poprvé přišla s principem rovnosti a rozlišených odpovědností. Rozvinuté země jejím prostřednictvím uznaly, že problém změny klimatu je především jejich zodpovědností, a proto by se také měly nejvíc podílet na jeho vyřešení. A přijaly odpovědnost nejen za snižování svých emisí, ale také za podporu rozvojových zemí při přechodu od fosilních paliv k bezuhlíkové ekonomice.

Jak ale napsal Gaurav Ganti, klimatický výzkumník na Humboldtově univerzitě, dnes už je jasné, že rozvinuté země selhávají nejen v oblasti klimatických opatření, ale i ve financování tohoto procesu. Což vede k tomu, že některé rozvojové země přišly s požadavkem uplatnit své právo na tzv. spravedlivý podíl zbylého uhlíkového rozpočtu. Rozvojové země jsou oblasti s historicky nízkými emisemi na obyvatele, a proto mají silný morální nárok na zbývající „uhlíkový prostor", připomíná Gaurav Ganti. Klimatologové proto vypracovali studii, která se zabývá tím, jak by vypadal tento „spravedlivý podíl" pro Afriku a Jižní Asii.

Jejich zjištění asi nejsou příliš překvapivá. Pokud všechny rozvojové regiony vyčerpají svůj spravedlivý podíl na „uhlíkový prostor", cíle Pařížské dohody v oblasti klimatu se stanou nedosažitelnými. A to i za předpokladu, že by rozvinuté země zvládly dosáhnout nejvyšších možných cílů při snižování emisí. Potřebujeme tedy, aby rozvojové regiony zvýšily své ambice. Jenže jejich ochota k tomu bude nejspíš záviset na odpovídající podpoře ze strany rozvinutých zemí, a to jak ve formě rychlejšího zmírňování dopadů globálního oteplování, tak i intenzivnějšího financování potřebných opatření v této oblasti. Hrozbou je totiž ještě vyšší teplota, jejíž dopady by se stupňovaly a neúměrně postihly zranitelné skupiny obyvatel, jež ke změně klimatu přispěly nejméně.

Před námi jsou tedy nesmírně složité otázky, jak problém vyřešit, píše Gaurav Ganti. Jestliže se nám nepodaří na ně odpovědět, jemně vyvážená architektura Pařížské dohody a jejích cílů se podle něj může zbortit.

Sdružení globálních firem chce dosáhnout dekarbonizace těžkého průmyslu

U problematiky změn klimatu ještě zůstaneme, tentokrát s poněkud optimističtější informací. Už víc než šedesát velkých globálních firem se připojilo k celosvětové iniciativě nazvané First Movers Coalition, jejímž cílem je dekarbonizace odvětví těžkého průmyslu a dálkové dopravy, která vytvářejí 30 % celosvětových uhlíkových emisí. Koalice se snaží využít kupní sílu svých členských společností k dekarbonizaci sedmi průmyslových odvětví, u nichž je to mimořádně obtížné: Jde o produkci hliníku, letectví, chemický průmysl, betonářský průmysl, lodní dopravu, výrobu oceli a nákladní dopravu.

Iniciativa spočívá zejména v tom, že se tyto firmy, ve spolupráci se Světovým ekonomickým fórem (WEF) a také se zvláštním vyslancem prezidenta USA pro klima Johnem Kerrym, zavázaly k nákupu zelených technologií v hodnotě 12 miliard dolarů. Budou tedy část průmyslových materiálů a dálkové dopravy, které potřebují, nakupovat od dodavatelů využívajících řešení s nulovými nebo téměř nulovými emisemi uhlíku. A to i za cenu vyšších nákladů.

Aby totiž bylo možné zmíněných sedm průmyslových odvětví dekarbonizovat takovou rychlostí, která je nutná k udržení tempa oteplování planety na úrovni maximálně 1,5 stupně Celsia, je zapotřebí nízkouhlíkových technologií, jež zatím nejsou konkurenceschopné. First Movers Coalition chce svými nákupy příslušný trh nastartovat, jinak řečeno posunout ho do bodu zlomu, který

zajistí cenovou dostupnost těchto technologií. Díky tomu budou podle WEF nové potřebné technologie k dispozici do roku 2030 a rozhodujícím způsobem přispějí k dosažení nulových emisí do roku 2050.

Na 30 % plochy oceánů vzniknou rezervace. Historická dohoda, kterou by měl ocenit každý

Za monumentální vítězství ve snaze o ochranu oceánů označila organizace Greenpeace nedávno na půdě OSN přijatou Globální smlouvu o oceánech, kterou skoro před dvaceti lety iniciovala. To hlavní, co smlouva obsahuje, je ustanovení, že do roku 2030 bude 30 % plochy oceánů chráněno prostřednictvím vytvoření sítě plně nebo vysoce chráněných rezervací ve všech oceánech. Dohoda se týká moří, která se nacházejí mimo jurisdikci národních států. Na nutnosti chránit 30 % oceánů a souše do roku 2030 se mezinárodní společenství shodlo již loni na podzim na konferenci o biodiverzitě COP 15 v kanadském Montrealu. Jak ale upozorňují představitelé Greenpeace, bez Globální smlouvy o oceánech tento cíl byl jen prázdným slibem bez možnosti jeho naplnění.

Někdo by možná namítl, že se nestalo nic světoborného a že jsou oceány důležité především pro oceánská společenství, takže nás se to až tolik netýká. Takové tvrzení by ale bylo pravdě hodně vzdálené. Dobrá kondice oceánů je totiž důležitá prakticky pro každého člověka na planetě.

Důvodů je pro to celá řada. Oceány jsou především klíčovým prvkem koloběhu vody a ovlivňují každodenní počasí i klima na celém světě. Jsou také hlavním zdrojem tzv. modrých potravin neboli potravin z vodních zdrojů, od kterých si navíc odborníci v příštích letech slibují výraznou pomoc v boji proti globální podvýživě a také významný vliv na růst kvality potravin. Například ve Spojených státech se mořské hospodářství podílí na HDP přibližně 361 miliardami dolarů a zaměstnává zhruba 2,2 milionu lidí.

Tím ale výčet zdaleka nekončí. Oceány také poskytují například polovinu kyslíku na Zemi a jsou bezkonkurenčním pohlcovačem uhlíku – pohlcují přibližně 25 % antropogenního uhlíku. A podle nových výzkumů může být tato hodnota dokonce o 9–11 % vyšší.

Globální ekonomické oživení na obzoru. Zatím je ale křehké, rizikem je hlavně ruská agrese

Podle statistik Organizace pro ekonomickou spolupráci a rozvoj (OECD) globální růst ekonomiky vloni celkem pochopitelně zpomalil. Výsledek v podobě 3,2 % je podle analytiků organizace výrazně pod očekáváním z počátku roku a je důsledkem ruské agrese na Ukrajině, krize v oblasti životních nákladů a také zpomalení v Číně.

Dnes už OECD upozorňuje na pozitivnější signály. Čína se zlepšovat podnikatelská a spotřebitelská nálada, ceny potravin a energií klesají a Čína se opět plně otevřela. V letošním a příštím roce by měl globální růst zůstat na úrovni 2,6 %, resp. 2,9 %. Očekává se ovšem postupné zlepšování s tím, jak bude ustupovat vliv vysoké inflace na příjmy. Konkrétně v eurozóně by měl růst letos dosáhnout 0,8 %, ale během příštího roku už téměř dvojnásobku, s tím, jak odezní vliv vysokých cen energií.

Právě inflace je téma, na něž je upřena pozornost celého světa. Ta celková už sice klesá, ale jádrová inflace zůstává zvýšená. Je to důsledek převážně silného růstu cen služeb, vyšších marží v některých odvětvích a také tlaků, které působí na náklady kvůli napjatým podmínkám na trhu práce. Podle analytiků OECD se v průběhu následujících dvou let inflace postupně zmírní, ale ve většině zemí zůstane nad cíli centrálních bank až do druhé poloviny roku 2024.

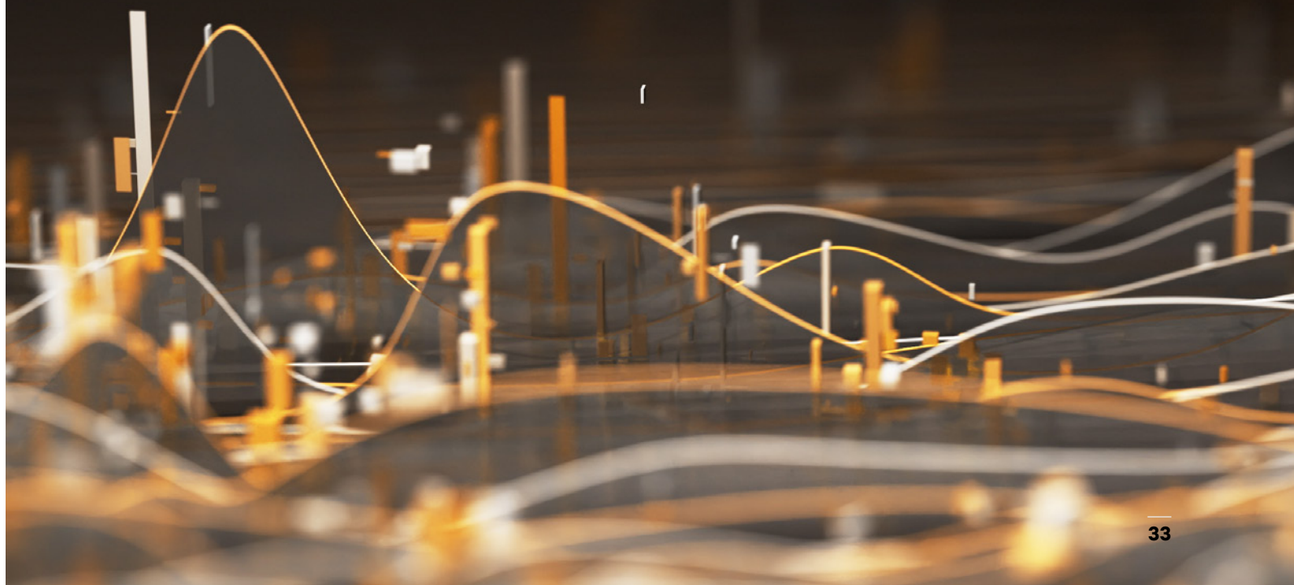
Zlepšení výhledu pak je podle nich stále křehké, a to především kvůli nejistotě ohledně průběhu války na Ukrajině a jejích širších důsledků. Hrozbou je také finanční zranitelnost plynoucí mj. z vysokého zadlužení či riziko znovuobjevení tlaků na globálních trzích s energiemi, což by mohlo vést k obnovení prudkého růstu cen a vyšší inflaci, píšou analytici OECD.

Proto podle nich musí měnová politika zůstat restriktivní, dokud se neobjeví jasné známky trvalého snížení základních inflačních tlaků. Také je potřeba, aby fiskální podpora s cílem zmírnit dopad vysokých cen potravin a energií byla víc zaměřena na ty, kdo to nejvíce potřebují. Nezbytné bude i provádění strukturálních reforem, zaměřených na zvýšení dynamiky podnikání, snížení překážek přeshraničního obchodu a ekonomické migrace a podporu flexibilních a inkluzivních trhů práce. A v neposlední řadě je zapotřebí posílit mezinárodní spolupráci v úsilí o překonání nedostatku potravin a energie, pomoc s obsluhou dluhů zemí s nízkými příjmy a dosažení koordinovanějšího přístupu k úsilí o zmírnění emisí uhlíku, zdůrazňuje OECD.

Zaznamenáníhodný komentář k současné a budoucí ekonomické situaci pronesla pro Český rozhlas bývalá zástupkyně České republiky ve Světové bance, ekonomka Jana Matesová. I ona považuje za hlavní hrozbu vysokou inflaci. Nicméně ekonomická recese podle ní může v dlouhodobém horizontu pomoci snížit míru konzumerismu. Podle Jany Matesové jsme si totiž zvykli fetišizovat ekonomický růst, a tak musíme vyrábět víc a víc, což je špatně. Stále nakupujeme nové a nové věci, i když to nepotřebujeme, a měli bychom v tom brzdit. Částečně i z bezpečnostních důvodů nemůžeme být závislí na zemích, které nás vyhlašují za své nepřátele, doplnila Jana Matesová.

Export Journal komentuje

Stále nakupujeme nové věci, které nepotřebujeme. I kvůli bezpečnosti bychom měli brzdit.



Zdroj: Midjourney

Umělá inteligence a naléhavé otázky

Velkým tématem současnosti se stává umělá inteligence (AI). Výsledkem čím dál vypjatějšího konkurenčního boje mezi hlavními vývojáři AI jsou stále dokonalejší tzv. velké jazykové modely (LLM, z angl. large language model) v podobě ChatGPT a dalších. Kromě nich ovšem tyto aktivity přinášejí také stále naléhavější otázky.

Nedávná výzva neziskové organizace Future of Life Institute zaměřené na zkoumání rizik umělé inteligence, která nabádá, aby byl vývoj na minimálně půl roku pozastaven a během této doby vypracována široce sdílená bezpečnostní pravidla, a kterou podepsal mimo jiné i Elon Musk, nejspíš není reálná. To ale neznamená, že o těchto aspektech nemá smysl diskutovat a pokoušet se o nalezení shody. Podle některých hlasů není třeba se umělé inteligence bát, protože už ji přece dnes používáme poměrně běžně. Jiní ale říkají, že stav, kdy jsou bezpečnostní záruky dány v podstatě jen tím, co nám výrobci nejnovějších jazykových modelů sami sdělí, je vysoce nežádoucí. A také že je možné, že výrobci LLM už vyvinuli pokročilejší systém, než je ten, který je dnes každému zdarma k dispozici. Systém AI, která nabyla vědomí, což by bylo skutečně přelomové.

Proto je jistě dobré, že vznikají iniciativy, které se pokoušejí sdružovat významné globální aktéry, společně diskutovat o důležitých souvisejících otázkách a hledat řešení. Například Světové ekonomické fórum v Globální akční alianci pro umělou inteligenci sdružuje více než 100 společností, vlád, organizací občanské společnosti a akademických institucí s cílem urychlit zavádění odpovědné umělé inteligence v globálním veřejném zájmu.

Například jeho Platforma pro utváření budoucnosti umělé inteligence a strojového učení se zaměřuje na urychlení procesu zavádění transparentní a inkluzivní umělé inteligence, tak aby bylo možné ji využívat bezpečným, etickým a odpovědným způsobem. Fórum mj. vytvořilo sadu nástrojů určenou organizacím, pracovníkům a společnosti obecně s cílem podpořit pozitivní a etické využití AI. Tvorbou AI standardů pro děti připravuje instrukce pro oblast vzdělávání a také pro podporu postavení a ochrany dětí a mládeže. Další platforma pak poskytuje praktické nástroje, které společnostem pomohou lépe pochopit etický a obchodní dopad jejich investic do AI, a ve spolupráci s britskou vládou vznikl soubor doporučení pro zadávání veřejných zakázek, jejichž cílem je umožnit využívání odpovědné AI ve veřejném sektoru atd.

Export Journal komentuje

Zastavit vývoj AI už není možné.

M, N

Slovníček pojmů pro zahraniční obchod

Margin
Marže vyjadřuje výnos z prodeje v procentech. Počítá se jako podíl mezi ziskem a prodejní cenou, přičemž zisk představuje rozdíl mezi prodejní a nákupní/výrobní cenou.

Maturity
Maturita neboli splatnost je datum, ke kterému končí daná obchodní transakce nebo finanční instrument. Využívá se například u dokumentárních plateb, bankovních záruk, půjček nebo produktů investičního bankovnictví (např. futures, opce).

Negotiation / Negotiating bank
Obecně se v bankovní praxi pojmem negociace označuje úplatný převod směnky. Pojem negociace je však používán také v oblasti trade finance, kdy je negociací nazýván jeden ze způsobů použitelnosti dokumentárního akreditivu. Jedná se o poměrně složitý způsob použití akreditivu typický především pro anglosaský svět, který spočívá v „odkupu“ směnky a/nebo dokumentů v rámci jejich prezentace pod akreditivem. U takto použitelného akreditivu zmocňuje vystavující banka jmenovanou banku k negociaci směnky, odpovídá-li podmínkám akreditivu. Jmenovaná banka, nazývaná také negociační banka, pak poskytne beneficientovi akreditivu platbu nebo závazek poskytnout platbu dříve, než obdrží akreditivní částku od vystavující banky.

Nominated bank
V oblasti trade finance se jako nominovaná banka označuje banka, u které je akreditiv použitelný, tj. banka uvedená v poli 41A akreditivní listiny. Nominovanou bankou může být také banka avizující akreditiv beneficientovi.

Nostro account
Nostro účet je účet vedený zahraniční bankou pro domácí banku, tj. například účet vedený německou bankou pro banku z České republiky. Nostro účet slouží především k realizaci přeshraničního platebního styku v cizích měnách.

Tiráž

Název titulu: Export Journal
Číslo vydání: 1/2023
Vychází: 30. 6. 2023
Registrace: MK ČR E 19644
Periodicita: 2× ročně
Ročník XIII
Vydavatel: Corporate Publishing, s. r. o.
U Golfu 565, 109 00 Praha 10, www.copu.cz
Produkce a grafické zpracování:
Corporate Publishing, s. r. o.
Redakce: Martin Zika, Jan Vejmělek, Tomáš Rak
Jazyková úprava: Proofreading.cz
Foto: Vojtěch Vlk, shutterstock.com, archivy firem a institucí
Produkce: Jiří Tingl – KB, Ditta Dvořáčková – CoPu
Inzerce: Ditta Dvořáčková, +420 603 196 614, ditta.dvorackova@copu.cz
Tisk: TNM PRINT, Nové Město 14, 503 51 Chlumec nad Cidlinou

Sídlo centrály Komerční banky:
Adresa: Na Příkopě 33 čp. 969, PSČ 114 07,
P. O. BOX 839, Česká republika
Informační linka KB: 800 521 521
Pro volání ze zahraničí: +420 955 559 550
www.kb.cz

Kontakt na Global Transaction Banking KB
Markéta Kryslová
manažerka GTB KB
tel.: +420 955 541 550
e-mail: marketa_kryslova@kb.cz
Václavské nám. 42, 114 07 Praha 1

Dotazy a připomínky můžete do KB zaslat elektronicky na e-mailovou adresu: mojebanka@kb.cz.


Banka
velkého byznysu
BUDOUCNOST
JSTE VY
KB