

## EKONOMIKA

## Hospodářský růst eurozóny ve 2. čtvrtletí zpomalil

Růst ekonomiky eurozóny i celé Evropské unie ve druhém čtvrtletí podle statistického úřadu Eurostat citelně zpomalil, v obou případech činil 0,2 procenta. V prvních třech měsících roku se HDP zemí eurozóny zvýšil o 0,4 procenta, v celé EU pak o 0,5 procenta. Zaměstnanost v eurozóně pak proti prvnímu čtvrtletí vzrostla o 0,2 procenta, v celé EU o 0,3 procenta. Mezi unijními zeměmi zaznamenalo nejvyšší mezičtvrtletní růst Maďarsko.

## BANKY

## ČR chce navýšit kapitál v bance pro obnovu a rozvoj

Česká republika plánuje navýšit kapitál v Mezinárodní bance pro obnovu a rozvoj (IBRD) o zhruba 546 milionů korun, a to pěti ročními splátkami po 109,1 milionu korun. Návrh dnes projedná vláda. V návrhu se uvádí, že zájmem Česka je usilovat minimálně o udržení svého současného postavení v IBRD a neoslabit tak svoji hlasovací sílu. Podle ministerstva financí představuje členství Česka v IBRD obchodní příležitost pro české podniky.

## AUTOBATERIE

## Škoda Auto vyrábí baterie pro elektromobily VW

Automobilka Škoda Auto vyrobila ve svém hlavním závodě v Mladé Boleslavi první sériové komponenty pro elektrické automobily koncernu Volkswagen. Vysokonapěťové baterie budou pohánět plug-in hybridy vycházející z modulární platformy MQB. Používat se budou například v modelu Škoda Superb iV, jehož výroba bude zahájena v závodě v Kvasinách. Počáteční výrobní kapacita je 150 000 kusů ročně.

## OBCHOD

## Alibaba kupuje za dvě mld. USD Kaola

Čínský internetový prodejce Alibaba Group se dohodl s čínskou herní společností NetEase, že od ní za dvě miliardy USD (46,8 miliardy korun) koupí internetový obchod Kaola. Ten se specializuje na prodej zahraničního luxusního zboží domácím spotřebitelům. Současně také Alibaba investuje 700 milionů USD do menšinového podílu divize NetEase pro streamování hudby.

# Únik dat vyjde firmy na miliony

PROBLÉMY S KRÁDEŽEMI DAT JSOU PRO FIRMY STÁLE NÁKLADNĚJŠÍ. ZA MNOHÉ ÚNIKY NEMOHOU HACKEŘI, ALE JEJICH VLASTNÍ ZAMĚŠTNANCI.

Adam Kotrbatý

adam.kotrbaty@economia.cz

**P**růmerný únik dat vysaje z firemních pokladen v celosvětovém měřítku desítky milionů korun. Do nesprávných rukou se takto dostávají například osobní údaje klientů, důležité databáze s obchodními kontakty i obsah firemních transakcí a komunikace.

Podle globální studie technologické společnosti IBM a organizace Ponemon Institute zaměřující se na kyberbezpečnost zaplatily firmy za jeden únik mezi červencem 2018 a dubnem 2019 v průměru 3,92 milionu dolarů (v přepočtu asi 90 milionů korun). Částka zahrnuje nejen hodnotu dat, ale také náklady na vyřešení incidentu a ztráty z odlivu klientů.

Problémem je i zvyšující se doba, za kterou jsou firmy schopny se s únikem vypořádat. Za poslední dva roky stoupla o 22 dní. Jen odhalení potíží trvá více než půl roku. Další desítky dnů potřebují společnosti na to, aby je potlačily. Podle studie se s rostoucím časem zvyšují i náklady. I proto nejvíce stojí úniky způsobené hackerskými útoky, škodlivým softwarem a zneužitím dat zaměstnanci.

## Rizikem jsou vlastní zaměstnanci

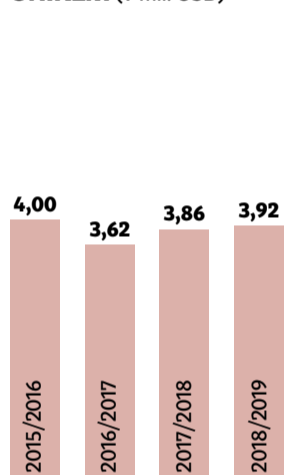
Jejich globální podíl Ponemon Institute a IBM vyčíslily na 51 procent všech případů. Zbytek si mezi sebe rozdělily závady na firemních systémech (25 procent) a lidské neúmyslné chyby (24 procent). „Zaměstnanec neví, jak se má chovat, a například použije vlastní flash disk k přenosu firemních dat. Následně jej někde nechá. Nebo se často stává, že udělá chybu v e-mailové adrese a pošle data jinam, než chtěl,“ přibližuje ředitel české společnosti Safetika specializující se na zabezpečení dat Petr Žikeš, jak takové selhání jednotlivce vypadá.

Jeho kolega ze Safetiky Matej Zachar dodává, že data často vynášejí přímo zaměstnanci. Hackeři tak nepotřebují využívat škodlivý software, ale sází na sociální inženýrství nebo infiltraci firem. Proti tomu se nedá bránit prostou instalací antivirového softwaru, i proto je takový postup lákavý. „Pro hackery je snadnou cestou nechat se v podniku zaměstnat a následně si odnést databázi,“ konstatuje Zachar. Data následně využívají pro vlastní podnikání.

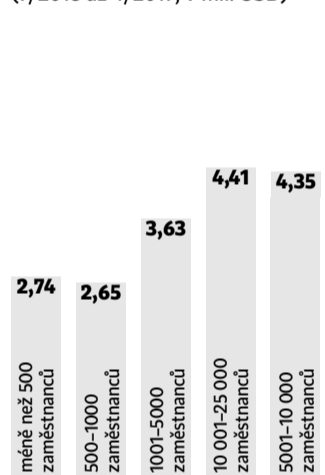
## KYBERÚTOKY SE NEVYHÝBAJÍ ANI ČESKU

Kybernetické útoky a s nimi související úniky dat připraví firmy v průměru téměř o čtyři miliony dolarů ročně. Nejpostiženější jsou velké firmy. Nejvíce dopadají úniky na podniky ve zdravotnictví.

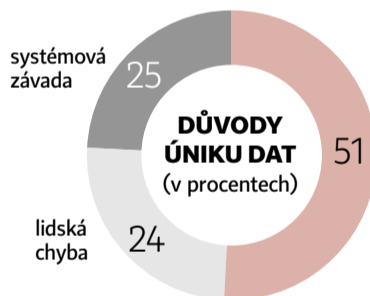
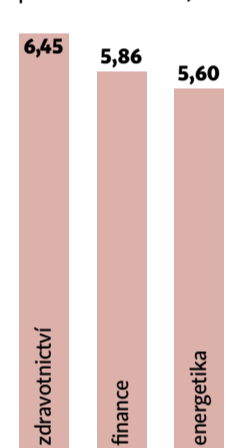
## PRŮMĚRNÉ ŠKODY ZPŮSOBENÉ DATOVÝM ÚNIKEM (v mil. USD)



## PRŮMĚRNÉ ŠKODY PODLE VELIKOSTI FIREM (7/2018 až 4/2019, v mil. USD)



## NEJPOSTIŽENĚJŠÍ ODVĚTVY (7/2018 až 4/2019, průměr v mil. USD)



útoky škodlivým softwarem a jiná kyberkriminalita (Firma stojí o čtvrtinu více než ty způsobené lidskou chybou či závadou systému.)

**8,19** milionu USD

jsou největší průměrné škody způsobené úniky dat v USA.

**25 %**

Čtvrtina českých firem byla v letech 2016–2017 obětí kyberkriminality.

## NEJVĚTŠÍ HROZBY PRO ČESKÉ FIRMY

**phishing** **malware**  
podvodné vylákání citlivých údajů a dat **útok škodlivým softwarem**

**6815** trestných činů

bylo spácháno v oblasti kyberkriminality a kriminality na internetu v roce 2018. Jde o meziroční nárůst 1161 činů.

V minulosti měly problémy s úmyslnými i nevědomými úniky dat například letecká společnost British Airways, internetový portál Reddit či oděvní firma Under Armor. V loňském roce musel masivní skandál se zneužitím dat řešit Facebook v rámci tzv. kauzy Cambridge Analytica.

Úniky se nevyhýbají ani českým podnikům. Pokutu 1,5 milionu korun dostal loni provozovatel internetového e-shopu Mall.cz, jemuž unikla data více než 700 tisíc zákazníků. Problém měl i dopravce Leo Express.

Také v tuzemsku jdou škody podle Safetiky do jednotek až desítek milionů. Přesná čísla o počtu útoků a škodách však nejsou k dispozici. „Firmy úniky často nemedializují, proto je složité informace získat. Když už k incidentu dojde, snaží se jej zvládnout interně. Ale můžeme říct, že úniky dat řeší desítky procent českých firem,“ vysvětluje Žikeš. Podle loňské studie, kterou každé dva roky vydává agentura PwC, se mezi lety 2016 a 2017 stala obětí kybernetické kriminality čtvrtina českých společností.

## Speciální tým ušetří i desetinu ztrát

Ponemon Institute a IBM doporučují firmám zřídit speciální tým, který bude na úniky dat reagovat. Uvádí, že takový krok v průměru ušetří asi 360 tisíc dolarů na případ, tedy zhruba desetinu z průměrných ztrát.

Únikům lze předcházet, pokud si firmy udržují o svých datech přehled, dbají na jejich šifrování a dostatečně školí své zaměstnance. V Evropské unii zavedlo povinnost data dostatečně zabezpečovat a mít přehled, kdo k nim má přístup, nařízení o ochraně osobních údajů známé jako GDPR, které platí od loňského května.

Péče o data se může vyplatit nejen firmám, ale také jednotlivcům. Na ně míří třeba podvodné e-maily, které se z nich snaží vylákat citlivé údaje (tzv. phishing). Ty mohou hackeři zneužít proti dotyčnému, například jej připravit o peníze.

Vedle phishingu je dalším rizikem stahování škodlivého softwaru. Ten se často skrývá v obrázku, v e-mailu, případně rovnou na webových stránkách. Takové útoky nelze stoprocentně vymýtit, ale jde se proti nim bránit právě dodržováním správných postupů. Mezi ně patří mimo jiné používání antivirových programů.

PÁNSKÁ MÓDA  
ŠITÁ NA MÍRU

**M**  
manemo

TEĎ JE ŘADA NA VÁS

Pštrossova 207/1, Praha  
www.manemo.cz

