



V aktuálním IT Kompasů jsme pro Vás připravili:

Vybrané aktuality ze světa IT

Tipy – Triky

Soutěž

Vtip pro dobrou náladu

207. číslo

Vybíráme zajímavé aktuality:

Ruští aktéři cílí na uživatele Signalu. NÚKIB vydává analýzu a doporučení, jak si aplikaci zabezpečit

Útočníci se nesnaží prolomit end-to-end šifrování aplikace Signal. [Více...](#)

Kyberzločinci útočí na školství, na darknetu obchodují s daty studentů i přístupy do škol

Check Point zaznamenal na darknetových fórech také obchodování s daty studentů a přístupy do vzdělávacích institucí. [Více...](#)

Více aktualit naleznete na www.AntiviroveCentrum.cz nebo na [Facebooku](#) .

Tipy a triky

Jak vybrat dokovací stanici?

Dokovací stanice přijde vhod ve chvíli, kdy notebooku přestanou stačit jeho vlastní porty. Umožní připojit monitor, klávesnici, myš, síťový kabel, tiskárnu, externí disk nebo další příslušenství a zároveň udržet na stole minimum kabelů.

Ne každá dokovací stanice ale zvládne totéž. Před nákupem je proto důležité ověřit především podporu monitorů, nabíjení a možnosti USB-C portu v notebooku.



Dokovací stanice

Dokovací stanice funguje jako rozbočovač mezi notebookem a připojenými zařízeními. Podle modelu může nabídnout USB-A, USB-C, HDMI, DisplayPort, LAN, audio konektor, čtečku karet nebo další porty.

Druhy dokovacích stanic:

USB hub: základní řešení pro několik portů navíc

USB hub je nejjednodušší a obvykle také nejlevnější varianta. Hodí se hlavně tehdy, když potřebujete několik USB portů navíc pro myš, klávesnici, flash disk nebo externí disk.

Na rozdíl od plnohodnotné dokovací stanice nemusí podporovat připojení monitoru, nabíjení notebooku nebo síťové připojení.

USB-C dokovací stanice: univerzální volba pro domácnost i kancelář

USB-C dokovací stanice nabízí kombinaci nejčastěji používaných konektorů – například HDMI, DisplayPort, USB-A, USB-C, Ethernet, čtečku karet nebo audio.

Pro většinu uživatelů jde o praktické řešení pro připojení monitoru, klávesnice, myši, internetu a dalšího příslušenství. Před nákupem ale ověřte, zda USB-C port notebooku podporuje také přenos obrazu a případně nabíjení přes Power Delivery.

Dokovací stanice s Power Delivery: jeden kabel pro data i nabíjení

Power Delivery umožňuje přes jediný USB-C kabel přenášet data a obraz a zároveň notebook nabíjet. Všechno ostatní tak může zůstat zapojené v dokovací stanici.

To je praktické především při střídání notebooku mezi domácím a pracovním stolem. Důležité je ale zkontrolovat výkon nabíjení – některé notebooky potřebují výrazně více energie než jiné.

Thunderbolt dokovací stanice: výkonné řešení pro náročné uživatele

Thunderbolt nabízí vysoké přenosové rychlosti a možnosti pro práci s více monitory, rychlými externími disky nebo náročnými periferiemi.

Tyto dokovací stanice bývají dražší než běžné USB-C modely, ale mohou být vhodné pro profesionální práci, například grafiku, střih videa, vývoj nebo práci s velkými soubory.

Univerzální a značkové dokovací stanice

Univerzální dokovací stanice jsou určeny pro různé notebooky a hodí se například do domácností nebo kanceláří, kde se používá více značek zařízení. Jejich kompatibilita ale nemusí být u všech funkcí stejná.

Výrobci notebooků zároveň nabízejí vlastní značkové dokovací stanice. Ty mohou nabídnout lepší kompatibilitu a jednodušší správu, jejich nevýhodou bývá vyšší cena a menší univerzálnost.

Přenosná a stolní dokovací stanice

Přenosné modely jsou malé a lehké, takže se hodí na služební cesty, prezentace nebo práci mimo kancelář. Obvykle nabídnou základní porty, jako HDMI, USB nebo USB-C.

Pro stálé pracovní místo je praktičtější větší stolní dokovací stanice. Ta může mít více portů, stabilnější napájení a umožní mít monitor, klávesnici, myš, síť i další příslušenství zapojené natrvalo. Notebook pak stačí připojit jediným kabelem.

Monitory s integrovanou dokovací stanicí: Vše v jednom těle

Stále populárnější alternativou ke klasickým krabičkám jsou monitory, které mají plnohodnotnou dokovací stanici zabudovanou přímo v sobě. K takovému monitoru připojíte klávesnici, myš, internetový kabel i sluchátka. Následně stačí k notebooku připojit jediný USB-C nebo Thunderbolt kabel, který se postará o:

- Přenos obrazu a zvuku do monitoru.
- Napájení a nabíjení notebooku (díky integrovanému Power Delivery).
- Připojení veškerého příslušenství zapojeného v zádech monitoru.

Toto řešení výrazně redukuje množství kabelů na stole a šetří finance i místo, protože nemusíte dokovací stanici kupovat samostatně. Stejně jako u běžných dokovacích stanic je ale potřeba si pohlídat, zda monitor dokáže dodat dostatek wattů (Power Delivery) pro nabíjení vašeho konkrétního notebooku.

Porty na dokovacích stanicích

Při výběru záleží především na tom, co budete připojovat. Mezi nejčastější porty patří:

- **USB-A a USB-C** – myš, klávesnice, flash disk nebo externí disk.
- **HDMI, DisplayPort, VGA nebo DVI** – monitor či projektor.
- **Audio** – sluchátka, mikrofon a další zvuková zařízení.
- **LAN** – stabilní připojení k internetu pomocí kabelu.
- **SD slot** – praktický například pro fotografy a tvůrce obsahu.

Výkon nabíjení

U dokovací stanice s Power Delivery si ověřte její maximální nabíjecí výkon ve wattech. Ten musí odpovídat požadavkům notebooku.

Výkon lze jednoduše vypočítat vynásobením napětí ve voltech a proudu v ampérech. Pokud dokovací stanice notebook neutáhne sama, může být stále použitelná, jen budete potřebovat samostatný napájecí adaptér.

Jak se v roce 2026 nejlépe chránit před kyberútoky?

Kybernetické hrozby se rychle mění a postupy, které stačily před několika lety, dnes nemusí být dostatečné. Útočníci stále častěji využívají automatizaci a umělou inteligenci, proto se vyplatí zaměřit na několik základních návyků.



1. Používejte správce hesel

Nepoužívejte stejné nebo podobné heslo na více službách. Pokud dojde k úniku hesla z jednoho webu, útočníci ho mohou zkoušet i u dalších účtů.

[Správce hesel](#) dokáže vytvářet dlouhá a unikátní hesla pro jednotlivé služby. Vy si pak musíte pamatovat pouze hlavní heslo.

2. Zapněte vícefaktorové ověřování

Vícefaktorové ověřování (MFA) přidává k heslu další způsob ověření. I při jeho odcizení tak útočník potřebuje ještě druhý faktor.

Pokud je to možné, používejte ověřovací aplikaci nebo bezpečnostní klíč. MFA zapněte především u e-mailu, bankovníctví, pracovních účtů a sociálních sítí.

3. Přemýšlejte, než kliknete

Phishingové zprávy jsou díky AI stále přesvědčivější. Dávejte pozor na naléhavé požadavky, podezřelé adresy odesílatelů, odkazy vedoucí jinam než na uvedenou stránku nebo nečekané přílohy.

Pokud si nejste jistí, neklikejte na odkaz v e-mailu. Web služby otevřete přímo zadáním její adresy nebo použijte oficiální aplikaci.

4. Aktualizujte software

Aktualizace často opravují bezpečnostní chyby, které mohou útočníci aktivně zneužívat.

Pravidelně aktualizujte operační systém, prohlížeč, mobilní aplikace, router i chytrá zařízení. Pokud je to možné, zapněte automatické aktualizace.

5. Zálohujte důležitá data

Ransomware může zašifrovat soubory a požadovat výkupné. Pravidelné zálohy proto patří mezi nejdůležitější ochranu dat.

Praktickým pravidlem je 3-2-1: mít tři kopie dat, na dvou různých typech úložiště a jednu kopii mimo hlavní zařízení nebo domácnost.

6. Zabezpečte domácí síť

Změňte výchozí heslo administrace routeru a používejte moderní zabezpečení Wi-Fi, ideálně WPA3, případně WPA2.

Pravidelně aktualizujte firmware routeru a zvažte samostatnou síť pro návštěvy nebo chytrá zařízení.

7. Pozor na podvody vytvořené pomocí AI

Deepfake videa, klonované hlasy a velmi přesvědčivé podvodné zprávy jsou stále dostupnější. Útočník může například napodobit hlas známé osoby a požadovat rychlou platbu nebo jinou akci.

U neobvyklých požadavků si informace ověřte jiným způsobem – například zavoláním přímo dané osobě.

8. Zkontrolujte nastavení soukromí

Sociální sítě, aplikace a další služby mohou shromažďovat velké množství osobních údajů. Ty mohou následně usnadnit cílené podvody.

Pravidelně kontrolujte, kdo vidí vaše příspěvky a osobní údaje, omezte zbytečné sledování polohy a zrušte oprávnění aplikacím, které už nepoužíváte.

9. Buďte opatrní na veřejné Wi-Fi

Veřejné sítě v hotelech, kavárnách nebo na letištích nemusí být důvěryhodné. Pro citlivé činnosti je bezpečnější použít mobilní hotspot nebo VPN.

Na veřejné Wi-Fi se vyhněte přihlašování k citlivým službám, pokud k tomu nemáte důvěryhodné zabezpečené připojení.

10. Sledujte svou digitální stopu

Osobní údaje se mohou objevit v uniklých databázích i bez vašeho vědomí. Vyplatí se proto čas od času zkontrolovat, zda se váš e-mail neobjevil v některém známém úniku.

K tomu lze využít například službu [Have I Been Pwned](#) , která umožňuje ověřit, zda se e-mailová adresa objevila v evidovaných únicích dat.

Zároveň kontrolujte své účty, přihlašovací údaje a další informace, které o vás internetové služby uchovávají. Pokud zjistíte únik, změňte příslušné heslo a nepoužívejte ho jinde.

Místo zapamatování konkrétních nástrojů je užitečné držet se čtyř jednoduchých pravidel:

- **Měňte** – měňte výchozí hesla, aktualizujte software a při podezření na únik změňte přístupové údaje.
- **Posilujte** – používejte silná a unikátní hesla, vícefaktorové ověřování a další dostupné bezpečnostní prvky.
- **Oddělujte** – nespojujte zbytečně pracovní a osobní účty a oddělujte například návštěvní či chytrá zařízení od hlavní domácí sítě.
- **Kontrolujte průběžně** – kyberbezpečnost není jednorázová záležitost. Pravidelně kontrolujte aktualizace, účty, nastavení soukromí, zálohy a případné úniky údajů.

Soutěž

Vyhodnocení minulé soutěže:

Na otázku z minulého vydání elektronického magazínu IT Kompas odpověděl správně a ze správných odpovědí byl vylosován pan J. H., kterému tímto gratulujeme k výhře softwaru [Sticky Password Premium](#) pro 1 PC na rok zdarma.

Otázka zněla:

Co znamená zkratka v IT bezpečnosti „CSRF“?

Správná odpověď měla být:

Zkratka CSRF znamená Cross-Site Request Forgery (česky něco jako podvržení požadavku mezi různými weby).

Jde o závažný typ kybernetického útoku na webové aplikace, při kterém útočník přiměje prohlížeč přihlášeného uživatele k provedení nechtěné akce na legitimním webu, aniž by o tom uživatel věděl.

Více informací naleznete [zde](#).

Nová otázka:

Co znamená v IT bezpečnosti pojem „Captive Portal“?

Ze správných odpovědí vylosujeme výherce, který od nás získá [Avast Premium Security](#) pro 1 PC na rok zdarma.

Odpovědi pište do 20. 10. 2026 na e-mail amenit@amenit.cz.

Správnou odpověď a výherce uveřejníme v příštím čísle. Pokud se chcete co nejdříve dozvědět, zda jste vyhráli, staňte se našimi přáteli na [Facebooku](#).

Vtip pro dobrou náladu

Běží zajíc lesem a na zádech táhne obrovskou litinovou pánvičku.

Potká ho vlk a diví se: „Zajíci, co to máš za podivný batoh?“

Zajíc hrdě odpoví: „To není batoh, vlku. To je můj hardwarový firewall proti tvým zubům. Funguje to skvěle, jenom mám trochu pomalejší odezvu při běhu do kopce.“

Vydání IT Kompasu od 1. čísla naleznete [zde](#).