Recenze **M1** | Nadčasový **design** | Distanční **výuka**
Příběhy na pokračování | Chrome, Safari a **certifikáty**

iPure.cz 164/2020, čtvrtý ročník | **Šéfredaktor a zakladatel:** Filip Brož
Redakce: Jan Březina, Jan Pražák, Marek Hajn, Daniel Březina, Jura Ibl, Karel Oprchal, Michael Vita, Jiří Matějka, Jan Netolička, Karel Boháček
Editor: Marek Nepožitek | **Překlad:** Ondřej Pikrt
Grafická úprava a sazba: Cinemax, s.r.o., www.cinemax.cz
iPurecz, s.r.o., IČ: 06481663 | **Kontakt:** redakce@ipure.cz

Prosinec je v plném proudu...

Editorial ■ Karel Boháček

... ačkoli za okny je zatím spíš listopadové počasí. A jak doznívá podzim a poslední listí padá ze stromů, doznívá i uvádění novinek od Apple. Po smršti z předchozích měsíců se zdálo, že už známe všechny produkty, ze kterých můžeme vybírat dárky pod stromeček, ale tu a tam se ještě nějaké to překvapení objeví. Tento týden Apple nakonec uvedl dlouho očekávaná velká náhlavní sluchátka AirPods Max, která se můžou v následujících měsících hodit nejen pro práci z domova a poslechu hudby při popíjení horkého čaje za dlouhých zimních večerů, ale snad i při mrazivých procházkách.

I když doba velí spíš nákupu dárků a pečení cukroví, věřím, že si najdete chvíli, abyste se v tom všem shonu zastavili a přečetli si další nabité číslo vašeho oblíbeného magazínu. Pokud snad zvažujete, že někoho obdarujete jedním z nových MacBooků s chipem M1 z dílny Applu, ale dosud jste váhali, snad vaše obavy rozptýlí Filipův článek o zkušenostech s používáním nového MacBooku Air. Musím vás však varovat, protože hrozí, že jej po přečtení půjdete hned koupit.

S Honzou se podíváme na nadčasovost designu Apple a dozvíte se nejen to, proč je design technologických produktů vlastně trochu věda a proč při pohledu na nové telefony iPhone vzpomínáme na ty z doby před 10 lety, ale také to, proč ani po několika letech neztrácí produkty Apple na své atraktivitě. Že má Apple vše kolem svých produktů promyšlené na dlouhou dobu dopředu, ukazuje i článek od Daniela, který vypichuje, jak některé funkce produktů Apple – podobně jako některé seriály a filmové ságy – musely nejprve připravit základy a na nich začít stavět, aby se ukázal jejich skutečný potenciál.

Nechybí ani tradiční užitečné tipy od Karla Oprchala, který si pro vás tentokrát přichystal pokračování o distanční výuce, kde dostanete další nálož informací o tom, jak se poprat se studiem z domova. Lenka pokračuje na téma bezpečnosti, tentokrát o tom, jak digitální certifikáty pomáhají zůstat v online světě v bezpečí.

Zbývá několik posledních dní roku 2020, který nebyl asi podle představ nikoho z nás, ale věřím, že jednou ze stálic, na které se můžete vždy spolehnout i v roce příštím, bude nejen pravidelnost, s jakou Apple vydává své produkty, ale i nové číslo iPure každý týden.

Za celou redakci iPure vám přeji příjemné čtení a co nejklidnější předvánoční období.

MacBook Air s M1
Budoucnost je tady!

Recenze ■ Filip Brož

Vůbec nevím, co k tomu napsat. Nový čip M1 v základním MacBooku Air mi zbořil veškeré ideály o nadupaném stroji. Trochu se stydím cokoliv psát, zvlášť když jsem před rokem v tuto dobu vychvaloval MacBook Pro 16". Ten samozřejmě i nadále používám, ale již 14 dní testuji nový MacBook Air s čipem M1 v základní konfiguraci. Doslova mi vyrazil dech, zvlášť při náročných operacích, jako je střih 4K videa nebo hraní her na plné detaily. Chci vám to vše ukázat.

Nemá smysl znovu opakovat, jak nový MacBook Air vypadá. Je totiž naprosto stejný, jako předchozí model, tedy z hlediska designu. Ano, máme zde stále „tlusté“ rámečky okolo displeje, obyčejnou kameru FaceTime a hliníkové tělo. Změnou je samozřejmě klávesnice a funkční tlačítka na horním řádku. Nově je zde například tlačítko pro režim Nerušit, což osobně vítám. Často ho používám.

Reproduktory hrají stále stejně, trackpad je stále stejně úžasný, alespoň z mého pohledu. K MacBooku jsem nikdy nepoužíval myš, protože jak říká klasik, nedává smysl. Uvnitř nenaleznete žádný větrák, takže MacBook Air je naprosto tichý. Při práci uslyšíte špendlík, který spadne na zem. A to je právě to, co je nejpodstatnější.

PROSTĚ TOMU NEROZUMÍM…

Možná to zní jako klišé a opakovaná fráze, ale tohle je nový začátek počítačů! Ať už přenosných nebo stolních. Když vidím, co dokáže 7jádrové GPU, a to je jedno jádro z výroby vypnuté, protože se prostě nepovedlo, tak nechci vidět, co zvládne příští rok vylepšený chipset v 16" MacBooku Pro nebo v Macu Pro. Nebudu jen fantazírovat, chci vám demonstrovat, co jsem na něm dělal.

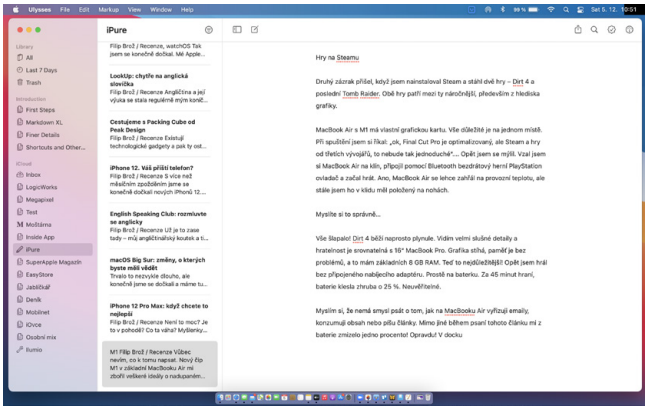
STŘIH VIDEA VE 4K

Hned první týden, co jsem měl náš redakční stroj u sebe, jsem dostal za úkol zpracovat Honzův videokurz o práci s iMovie, který se stal velmi úspěšným na Startovači a již nyní si videa můžete stáhnout a pustit. Byl jsem i u natáčení, které jsem odbavil na novém Canonu EOS R6. Honza si záznam zvuku dělal do drátového klopáku, který vedl k jeho iPhonu. Zároveň s tím dělal ve 4K videozáznam svého 16" MacBooku Pro, na kterém demonstroval výuku v iMovie.

Celkově jsem na MacBooku Air v aplikaci Final Cut Pro zpracoval 13 výukových videí, kdy každé z nich obsahovalo multicam a celkem jednoduchý střih. Zabralo mi to dva dny práce, přičemž (teď se něčeho chytněte) jsem celou dobu stříhal bez napájecího adaptéru a za tu dobu jsem MacBook Air nabil pouze dvakrát!!!

Čtete správně. Dvakrát. Celou dobu jsem ve Final Cut Pro stříhal bez nabíječky, vše jelo na baterii. K tomu jsem měl puštěné nějaké základní aplikace – Mail, Safari, Tweetbot, Apple Music a samozřejmě připojený externí SSD, na kterém jsem stříhal.

Celou dobu jsem stříhal videa doslova s MacBookem na klíně a kde se mi zachtělo. Jednou jsem seděl u stolu, pak jsem si sedl na gauč, do křesla a jednou i do postele. MacBook Air se za celou dobu



ani nezahřál! Když to srovnám se svým 16" strojem, na kterém jsem podobným způsobem připravil již stovky videí, tak by mi podobné workflow neprošlo.

Ta samá práce na 16" MacBooku Pro by v praxi znamenala, že bych musel mít připojený adaptér a být s ním u stolu. Kdybych si „pročko“ položil na kolena, možná bych musel za chvíli navštívit lékaře s drobnými popáleninami. Samozřejmě lehce přeháním, ale sami to znáte. A to nemluvím o větrácích, které se spustí už když Final Cut Pro spustíte.

Práci ve Final Cut Pro na MacBooku Air s čipem M1 bych přirovnal k iPadu Pro. Na tohle jsem byl celkem zvyklý, ač si myslím, že výdrž baterie na iPadu není tak vysoká. Samozřejmě je potřeba počítat s tím, že iPad Pro už nějakou dobu používám a baterie rozhodně nevydrží tolik, co na začátku. Podobné to bude i u MacBooku Air. Stárnutí baterie nezastavíte.

Tak či tak, na takovouhle práci jsem fakt nebyl zvyklý. Stříhal jsem 4K video ve Final Cut, jako kdybych odepisoval na emaily… prostě vše šlapalo. Žádné duhové kolečko, přehřívání či něco podobného. Prostě to šlapalo.

HRY NA STEAMU

Druhý zázrak přišel, když jsem nainstaloval Steam a stáhl dvě hry – Dirt 4 a poslední Tomb Raider. Obě hry patří mezi ty náročnější, především z hlediska grafiky.

MacBook Air s M1 nemá dedikovaný grafický adaptér. Vše důležité je na jednom místě, GPU je součástí čipu M1. Při spuštění jsem si říkal: „OK, Final Cut Pro je optimalizovaný, ale Steam a hry od třetích vývojářů, to nebude tak jednoduché.“ Opět jsem se mýlil. Vzal jsem si MacBook Air na klín, pomocí Bluetooth připojil bezdrátový ovladač z PlayStationu a začal hrát. Ano, MacBook Air se lehce zahřál na provozní teplotu, ale stále jsem ho měl v klidu položený na nohách.

MYSLÍTE SI TO SPRÁVNĚ…

Vše šlapalo! Dirt 4 běží naprosto plynule. Vidím velmi slušné detaily a hratelnost je srovnatelná s 16" MacBookem Pro. Grafika stíhá, paměť je bez problémů, a to mám základních 8 GB RAM. Teď to nejdůležitější! Opět jsem hrál bez připojeného nabíjecího adaptéru. Prostě na baterku. Za 45 minut hraní, klesla kapacita baterie zhruba o 25 %. Neuvěřitelné.

Myslím si, že nemá smysl psát o tom, jak na MacBooku Air vyřizuji e-maily, konzumuji obsah nebo píšu články. Mimo jiné během psaní tohoto článku mi z baterie zmizelo jedno procento! Opravdu! V docku mám přitom zapnuté další aplikace.

Vyzkoušel jsem také aplikace z iPhonu/iPadu. Fungují naprosto slušně, jen samozřejmě musíte

počítat s chybějící optimalizací některých tlačítek a prvků. Na druhou stranu, už je zde spoustu aplikací, které podporují čip M1 a nový macOS Big Sur. Každý den se přitom objevují nové.

PRO KOHO?

Chtěl bych napsat, že MacBook Air je naprosto pro všechny – náročné uživatele i obyčejné. Musím však být střízlivý, protože například pro vývojáře může představovat M1 v počítači problém z hlediska podpory aplikací. To samé platí, pokud chcete používat Windows. Raději počkejte. Pokud potřebujete nějaké speciální aplikace, které běží například v Javě nebo pod Rosetou, opět bych raději počkal.

Jestli naopak využíváte aplikace pro macOS, píšete, konzumujete, upravujete fotky, stříháte video a chcete MacBook Air pro osobní potěšení a práci, tak budete nadšeni. MacBook Air se v podstatě výkonnostně vyrovná MacBooku Pro. K tomu získáte tenké tělo, které je ultra-přenosné a vydrží neskutečný nápor na jedno nabití. Tentokrát čísla Applu opravdu nelhala. Na 18 hodin se lze opravdu dostat.

Rozdílem mezi MacBook Air a MacBook Pro v provedení M1 je opravdu jen výdrž baterie a ventilátor, který v případě MacBooku Pro dokáže dlouhodoběji zajistit plný výkon při nějaké náročné operaci. U Airu výkon prostě spadne, pokud dojde k maximálnímu

Rozdílem mezi MacBook Air a Pro s M1 je opravdu jen výdrž baterie a ventilátor, který MacBooku Pro dokáže dlouhodoběji zajistit plný výkon při nějaké náročné operaci.

zatížení, protože se systém nemá jak chladit. Na druhou stranu, ruku na srdce, kdo z nás opravdu potřebuje nepřetržitý maximální výkon? Já ne!

ČEKÁ NÁS ZAJÍMAVÁ BUDOUCNOST

Opravdu moc se těším, na další verze čipu M1, ať už se bude jmenovat jakkoliv. Myslím si, že bude neskutečně nabušený, a když vidím, co dokáže MacBook Air se sedmi jádry v základním provedení s 8 GB paměti, tak nebudu daleko od pravdy, že M1 udělá z Macu Pro raketoplán! Začíná se psát nová budoucnost počítačů a jsem rád, že mohu být na jejím počátku.

MacBook Air tak budu i nadále používat jako cestovní a druhé zařízení. V žádném případě nedávám sbohem své milované šestnáctce. Na druhou stranu – chci testovat aplikace pod M1, chci vytěžit maximální výkon při používání tohoto zařízení. Kdo jde do toho se mnou?


PORSCHE

Skvělý design je nadčasový

Magazín ■ Jan Pražák

Ačkoli se prodeje iPhonu řady 12 teprve pořádně rozjely, mnozí z nás si vzpomínají, na úžasný design iPhonu 4. Přestože se jedná o zařízení představené před více než 10 lety. Nové modely totiž přináší něco, co si zaslouží nebývalou pozornost.

Víte, že jsme se tématu designu již dotkli v našem dřívějším vydání. To se ale týkalo převážně pohledu na nehmotnou softwarovou část. S letošními iPhony mě však daleko více zaujala i fyzická stránka.

Kritici často komentují to, že Apple nedokáže pořádně inovovat vzhled opravdovou revolucí a tábor nadšenců zase chválí, jak je firma skvělá, že se vrátila k něčemu osvědčenému. Hranatý vzhled telefonů se jednoduše po dekádě vrátil zpět. Oběma skupinám ale uniká to zásadní – skvělý nadčasový design nepotřebuje pravidelnou obměnu.

JÁDRO

Samozřejmě potřebuje drobná vylepšování, vyhlazování maličkostí a zapracování nových materiálů. V jádru ale zůstává stejný. Nedávno jsem četl moc zajímavé přirovnání iPhonu k automobilům Porsche nebo klasickému fotoaparátu Leica.

Za sebe mohu říct, že se mi Porsche jako takové nikdy moc nelíbilo. Jsem příznivcem aut typu Mini nebo „běžných“ Škodovek. Proto jsem o spojení se sportovní značkou přemýšlel. Často mi právě přišlo, že Porsche jako jedna ze značek vlastně nevytváří nic nového. Opak je přitom pravdou.

ROZPOZNATELNOST

Díky tomu, že stále jen mírně vylepšují tradiční vzhled, je jejich typický designový prvek daleko nadčasovější, než kdyby každých několik přišla kompletní změna. Když si otevřete jejich stránky, všechny modely působí stejným dojmem. Liší se pouze cenou a velikostí. Porsche jednoduše poznáte kdekoli na silnicích. I v případě, že jej zahlédnete na dálnici ve zpětném zrcátku, víte, o jaké auto se jedná. Pak pokorně změníte pruh na pravý.

Když vám ale do zrcátka budou svítit světla Kodiaqa, Atecy nebo Touarega, nejspíš je na první dobrou od sebe nerozeznáte. A v tom je ta základní myšlenka. Pokud se vám povede vytvořit jakýkoli produkt, kde je design perfektně promyšlen, není třeba jej měnit každý rok nebo dva. Pokud tuto myšlenku dokončíme, dalo by se říct, že design iPhonu 4 zůstal dokonalým a posledních deset let bylo pouze hledáním nových možností, které nevyšly.

DĚDICTVÍ

Podobně je to s fotoaparáty Leica. Pokud vás někdo bude fotit v ateliéru, kde na vás budou mířit softboxy, asi úplně nepoznáte, zda na stativu před vámi stojí Canon nebo Nikon. Když si ale fotograf přinese Leicu, okamžitě poznáte, že je něco jinak. Každý produkt na světě přináší buď čest jménu své firmy nebo rozpačité pocity. iPhone 12 by se dal označit za produkt „dědictví“ Apple.

Místo iPhone 12 (s mnoha přídomky) jsme dnes také mohli mluvit o generaci iPhone Heritage. Jedná se totiž o částečný návrat ke kořenům, ale také o nadčasový design. O okamžité rozpoznání vzhledu mobilního telefonu, který na první pohled dokážete rozeznat od veškeré konkurence. Alespoň na dalšího půlroku, než dorazí konkurence s novými modely.

ŠIROKÝ VÝBĚR

Tím nechci myšlenku zjednodušit na to, že u iPhonu nemáte na výběr. U Porsche si taky můžete vybrat, zda chcete řídit sporťák 911 ve stříbrné nebo SUV Cayenne v červené. I u iPhonu 12 si můžete vybrat, zda chcete menší rozměry nebo sportovnější verzi Pro.

Pokud se ale na modelové řady obou firem podíváte najednou, uvidíte jasně daný základ, který se tolik neliší. A pokud nebudeme počítat různé sportovní úpravy nebo kabriolety, základních modelů má automobilka pouze šest (718, 911, Panamera, Taycan, Macan, Cayenne). Apple nabízí iPhone 12, 12 mini, 12 Pro, 12 Pro Max, SE druhé generace a starší iPhone 11 a XR. Kromě 4,7" SE však všechny telefony nabízí stejný způsob ovládání a velmi podobný vzhled.

Pokud si postavíme vedle nejnovějších modelů Porsche pouze nejnovější modely iPhonu, dostaneme jasný signál jednotného designového jazyka. Stejně jako tvůrce sportovních automobilů i Apple vylepšuje iPhone uvnitř a omezuje se jen na drobné změny ve vzhledu.

DLOUHOVĚKOST

Je také zajímavé, že se Apple snaží držet podobný vzhled po delší dobu (alespoň v rámci dnešního rychlého technologického vývoje). První model 911 opustil továrny Porsche ve Stuttgartu v roce 1964. Až do roku 1989 se nijak výrazně nelišil vzhledem.

Podobně iPhone 4 nastolil nové pořádky pro vzhled chytrého mobilního telefonu. Sám Steve Jobs si jej pochvaloval slovy: „Bezpochyby se jedná o nejpreciznější produkt, který jsme kdy vyrobili. Je také tou nejnádhernější věcí. Sklo na přední i zadní straně s hliníkovým rámečkem kolem dokola. Připomíná mi svou krásou staré fotoaparáty Leica.“

Letos bychom se dopočítali, kolik produktů čerpalo z tohoto převratného produktu z roku 2010. Jen pro pořádek celá nová generace iPhone 12, iPad Pro a také iPad Air. Můžeme jen spekulovat, zdali se k nám někdy dostane v hranatém vzhledu i iPad a iPad mini.

> „Bezpochyby se jedná o nejpreciznější produkt, který jsme kdy vyrobili. Je také tou nejnádhernější věcí. Sklo na přední i zadní straně s hliníkovým rámečkem kolem dokola. Připomíná mi svou krásou staré fotoaparáty Leica.“ (Steve Jobs)

iPhone 4 byl také převratným modelem v oblasti mobilní fotografie. Podobnost s iPhonem 12 tu bude i v tomto ohledu. Nové možnosti čoček ve spolupráci s umělou inteligencí opravdu konečně dávají možnost fotit v noci či pořizovat videozáběry v až filmové kvalitě.

Ne každý je vzhledem nadšen. Často v nás konkrétní vzhled vytváří buď pozitivní, nebo negativní pocity. Buď se nám něco líbí, nebo to obdivujeme, anebo na druhou stranu v nás něco drobného může vytvářet pocit strachu a úzkosti.

NEZŮSTANEME U ČTYŘ

Abychom celé kolo uzavřeli, je důležité připomenout následující řadu. Od iPhone 5 až po iPhone SE je vlastně tím, který postavil ty největší základy letošních novinek. iPhone SE první generace zdokonalil vše, co přinesly modely před ním. Rychlost otisku prstu, rychlost samotného zařízení, nádherný displej, rychlost internetového připojení, překvapivou výdrž baterie a skvělý fotoaparát. To vše v kombinaci s tělem, které se pohodlně drželo v jedné ruce.

V dnešní době zvětšování chceme vždy to největší, protože jsme přesvědčeni, že s menším zařízením nedokážeme být stejně efektivní. Ano, někdy to může být i pravda. Často je to ale spíš jen o marketingovém tlaku firem a našeho okolí.

Když si ale jdete do obchodu koupit oblečení (v současnosti spíše online), nevyberete si největší triko jen proto, že je největší. Vyberete si velikost, která vám sedí na vaši postavu. Podobně je třeba přemýšlet při výběru nejnovějšího modelu telefonu. Možná vám vaše prsty za váš výběr za pár let poděkují. Nebo vám poděkuje váš nadřízený, že jste skutečně efektivní na těch největších zařízeních, která Apple nabízí.

Evidentně je však iPhone ve stejné kategorii jako Porsche. Ne proto, že byste s ním mohli jezdit po dálnici 200 km/h, ale proto, že skvělý design je jednoduše nadčasový.

Distanční výuka s odstupem času

Magazín ■ Karel Oprchal

Všem nám je jasné, že tento semestr už dokončíme distančně. Všichni už také počítáme s tím, že i letní semestr dost možná začneme rovnou distanční formou, protože předpovídat v této době budoucnost vzdálenou dva měsíce se zdá být bláhové. Domnívám se, že tyto zkušenosti nevyhnutelně změní náš pohled na osobní setkávání a jeho důležitost. A pochopitelně se to dotkne i výuky, která stoprocentně bude probíhat mnohem častěji distančně než doposud.

Hned vysvětlím, proč si nemyslím, že je moje celkem odvážné tvrzení docela blízko reality. Když jsem posledně sepisoval své dojmy z distanční výuky, byl jsem tehdy pouze student, který nemohl chodit do školy. Do tří týdnů po zveřejnění toho článku jsem ale i jako lektor musel zvolit vhodné virtuální řešení svých kurzů, protože firmy, kde učím, zakázaly vstup cizích lidí, případně kompletně přešly na home office. Se svými studenty jsem se tedy rázem začal stýkat přes Zoom a v cestě nám tak nestála žádná překážka, aby výuka dál neprobíhala. Zde je vidět zřetelný posun oproti jarní vlně, kdy se stoplo de facto všechno. Rozdíl v mém životě nastal ten, že jsem rázem úplně přestal opouštět svůj domov narozdíl od vycházení několikrát týdně. Ne jen, že tak mám jednoznačně nulové riziko nákazy, protože všichni doma pracujeme online, ale člověk zjistí, že pokud si to dobře zařídí, má práci, kontakt s lidmi (byť jen přes kameru) a pokud si naplánuje pohyb na čerstvém vzduchu, dá se tak docela slušně fungovat. A člověk ani nezvlčí, protože má režim, s lidmi se stále vídá a musí se oblékat, česat, ženy líčit apod. Což mě docela děsí. Výhody jsou totiž jak ekonomické, tak praktické. Nemusíte startovat auto a ani nikam dojíždět, tím pádem vyděláváte stejně nebo srovnatelně a přicházíte o znatelně menší

množství peněz i času. Ten můžete třeba věnovat spánku, pokud jste měli perný den.

DISTANČNÍ VÝUKA JAKO ALTERNATIVA

Výsledkem toho je, že když je teď všechno jakž takž uvolněné, žádná z těch firem, které omezily kontakty, se úplně nemá k obnovení fyzické výuky. Proč? Protože vidí, že výhledy jsou docela bledé, že se stejně beztak k sociálnímu distancování vrátíme, tak proč pořád měnit způsoby jako ponožky. Je zde snaha o konzistentní, dlouhodobé řešení a já tomu rozumím. Faktem totiž je, že pokud se všechno dobře zorganizuje, jakákoli komunikace mezi dospělými může probíhat jakoukoli distanční formou, a bude to fungovat. S dětmi je to ale pochopitelně mnohem horší.

Pořád si stojím za tím, co jsem ve svém říjnovém článku napsal, protože při osobních setkáních funguje chemie a vnímání podstaty toho, co děláme, úplně jinak. Přesvědčit děti, aby výuku přes počítač braly vážně, když u sebe v pokoji mají tisíce dalších vjemů, které je rozptylují, je takřka nemožné. Jako studentovi mi distanční výuka s mnohými učiteli nevyhovuje, protože si nemyslím, že v tom umí chodit. Jsou to ale učitelé, jejichž výuka odjakživa patřila k těm méně zajímavým, tudíž je to přes počítač ještě horší. Nicméně jako učiteli a milovníku technologií mi výuka přes počítač dělá mnohem menší problém, než jsem čekal, a myslím, že mí studenti to taky nenesou vyloženě špatně. Proto bych se vůbec nedivil, kdyby současný boom distanční výuky neskončil bankrotem konferenčních platforem, ale naopak vyústil ve větší poměr distančně odučených či odpracovaných hodin k počtu hodin odučených nebo odpracovaných fyzicky, protože se prostě občas dva lidi shodnou, že je lepší komunikovat na dálku, než se někam zbytečně trmácet. Pokud to budeme brát tímto, dle mého názoru zdravým, způsobem a nebudeme distanční výuku upřednostňovat, nýbrž ji brát jako regulérní alternativu k fyzickému setkání, lidsky se posuneme dál a otevřeme si dveře k novým možnostem. Nakonec naše redakce tvoří magazín iPure, portál Digit, podcasty, Moštárnu a další projekty z 98 % distančně a funguje to docela obstojně, ale asi bych nás označil spíš za světlou výjimku, protože ne všechno může vznikat pouze po internetu.

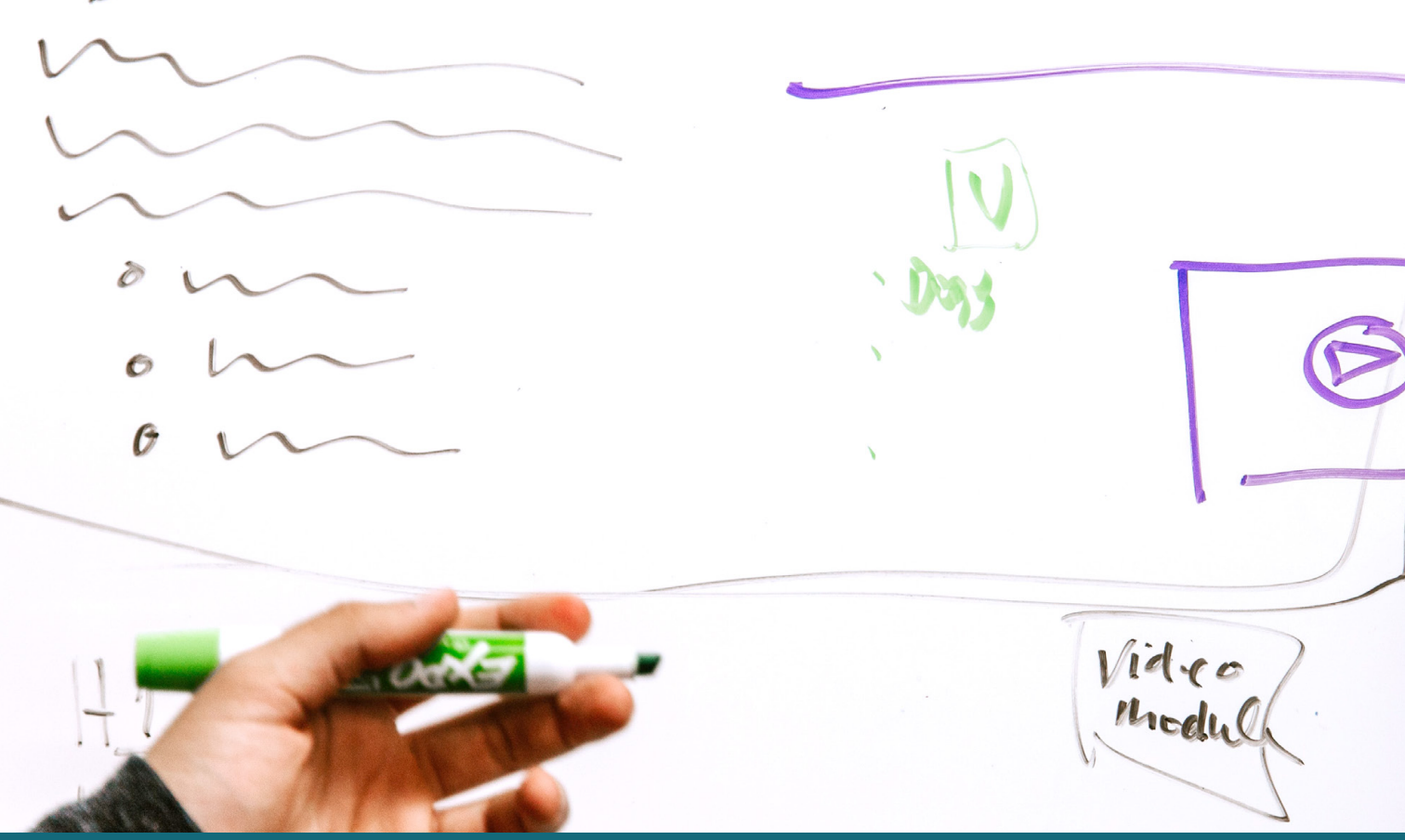
VYTĚŽIT NA MAXIMUM

Stav je, jaký je, a když už je potřeba přejít do režimu online, musí se to dělat naplno. Cílem přeci je i v této době fungovat jen s nejnutnějšími omezeními, protože omezení brzdí potenciál a výkon. Proto skutečně záleží na dobré volbě platformy, přes kterou se s ostatními stýkáte, a tuto platformu je dobré umět ovládat. Jak jsem posledně uvedl, ve škole máme zkušenost s open source řešením BigBlueButton a platformami Zoom a MS Teams. Kromě toho škola mé sestry zvolila pro distanční výuku řešení Jitsi Meet, které je podobné BigBlueButton, dá se učit přes Google Meet, pokud jste fanoušky Googlu, a využít se eventuálně dá i Skype. Osobně bych vyloučil FaceTime a jiná telefonní řešení, protože takhle nemůžete sdílet obrazovku, zvuky, soubory a jakkoli korigovat průběh setkání, což je docela podstatné.

Já jsem si už během distanční výuky na univerzitě hned z několika důvodů oblíbil Zoom. Je nejpřehlednější, nejméně náročný na hardware, síť i vaši gramotnost, od posluchače nevyžaduje registraci, je naprosto spolehlivý a primitivní, což je výhoda. Ne nadarmo se aplikace Zoom stala letošním vítězem ceny App Store Nejlepší aplikace pro iPad. Zoom je přesně to, co jako lektor cizích jazyků potřebuji. Spolehlivé řešení, možnost připojit se z telefonu, počítače i tabletu přes aplikaci i web, a především jednoduché připojení pro mé studenty. Nechci, aby se kvůli mému kurzu trápili zakládáním e-mailových adres, propojováním účtů a dalšími komplikacemi, které vyžadují MS Teams. Potřebujeme se připojit a jít na věc. MS Teams je komplexní řešení pro školní třídy a velké týmy v korporátních společnostech, kde se dají perfektně sdílet soubory, plánovat projekty, komunikovat v týmu anebo jen jako jednotlivci – v tom určitě nemají Teams konkurenci. Jenže pro mé využití mi to přijde zbytečné a navíc jsme já i mí kolegové ve škole několikrát narazili na to, že se nám zasekla spuštěná kamera a nebylo nás tím pádem vidět, nebo naopak se nám obraz jevil jako zaseklý, ale druhá strana nás viděla, navíc někteří spolužáci mají často problémy s připojením se do hovorů. Řešením je buď restartovat program, nebo rovnou celý počítač. Takovému riziku se já jako lektor vystavovat nemůžu.

> Už během distanční výuky na univerzitě jsem si oblíbil Zoom. Je nejpřehlednější, nejméně náročný na hardware, síť i vaši gramotnost, od posluchače nevyžaduje registraci a je naprosto spolehlivý.


wenn ich jemanden
hätte finden können,
damit er für mich sorgte.
konjunktiv.pdf - Adobe Acrobat Reader DC
Doplňte tvary konjunktivu perfekta
wenn ich jemanden
hätte finden können,
damit er für mich sorgte.
harman/kardon
OMEN



Zaplatil jsem si tedy licenci Zoom Meetings Pro, abych mohl organizovat hovory pro několik uživatelů najednou, nemusel se ničím omezovat, a plynule jsem se všemi svými tehdejšími kurzy přešel na distanční výuku. Tato licence vyjde s daní (objednává se na Zoom.us, kde jsou ceny bez daně) na necelých 17 EUR měsíčně, což v přepočtu vyjde na zhruba 470 Kč podle současného kurzu. Je to nejlevnější licence, kterou Zoom nabízí, a je pro mé potřeby zcela dostačující. Uživateli je vygenerováno tzv. Meeting ID, pomocí něhož organizujete své schůzky. Zvolíte si jednoduché heslo a hovor může začít jedním kliknutím na tlačítko Start Meeting. Schůzky se přes Zoom dají i plánovat a synchronizovat s vaším kalendářem, pomocí něhož můžete účastníky zvát, takže všichni dostanou před začátkem upozornění, a existují i další vychytávky. Já ale schůzky pouze spouštím a povoluji účastníkům se do mé místnosti připojovat i beze mě, víc nepotřebuji. Výuka se navíc často přesouvá a plánovat si do Zoomu schůzky je pro mě zbytečné. Ve škole heslo k výuce přes Zoom nepoužíváme, takže škola pravděpodobně využívá nějakou jinou licenci. Je samozřejmě na každém, k jakým účelům chce Zoom používat. Možností předplatného je celá řada, a pokud chcete jednoduché a funkční řešení pro jen pár nebo i několik tisíců lidí, mohu Zoom jen doporučit.

Aby ale vaše schůzky byly co nejblíže fyzickým setkáním, je nutné podotknout, že by si účastníci hovorů měli zapínat své kamery. Naprosto rozumím, že je vhodné vypínat si mikrofon, aby se při setkáních s padesáti lidmi účastníci navzájem nerušili šustěním a kašláním, ale zapnout si kameru by podle mě mělo být automatické. V rámci mých hodin s tím problém nemám, studenti vždy měli kamery zapnuté, ale ze zkušenosti s přednáškami a semináři na univerzitě i s distanční výukou mé mladší sestry vím, že si kameru zpravidla zapíná jen učitel, a mnohdy ani to ne. Přitom máme semináře, jejichž vedoucí si kameru vyžádali, a ta hodina má pak úplně jinou atmosféru, když vidíte, že za těmi avatary skutečně někdo sedí! Já si zapínám kameru vždy, a přestože se jedná o globální problém, nerozumím, proč se lidi nechtějí na kameře ukazovat. V angličtině dokonce existuje slovní spojení „camera-shy“ a Zoom ho ve svých newsletterech používá k motivaci lidí nebýt při schůzkách němí a neviditelní. Tak se nestyďte a zapněte si na příští schůzce kameru. Věřte mi, bude to mnohem lepší.

VÝUKA STOJÍ NA IPADU

Těžištěm mé výuky je iPad s Apple Pencil. Používám ho jak v každé hodině na univerzitě, tak v každé hodině, kterou sám vedu. Ve fyzických hodinách ho používám jako zdroj svých podkladů, jdu přes něj

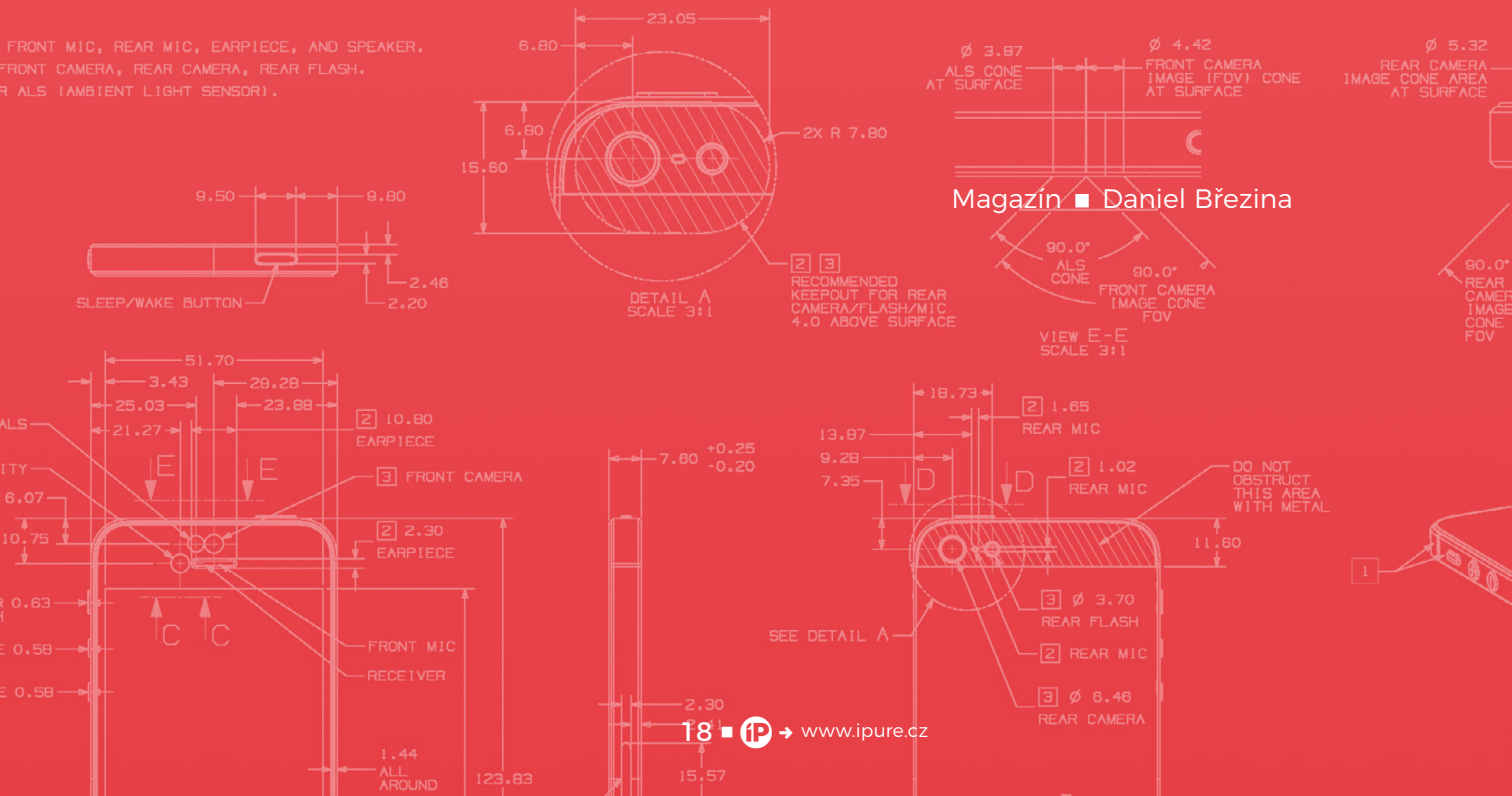
na internet a je to i tabule na psaní, když potřebuju studentům napsat nějaké poznámky. Apple se opět neplete; iPad neuvěřitelně obohacuje každou hodinu a pro toho, kdo to zkusí, bude iPad nenahraditelným společníkem, bez kterého si školu už nedovede představit.

A když jsem zvyklý iPad používat normálně, bylo by přece zvláštní, kdybych ho nezužitkoval i v distanční výuce. Mé vysílání probíhá ze dvou zařízení – z počítače a z iPadu. Na obou zařízeních mám staženou aplikaci Zoom Cloud Meetings a jsem přihlášen svým účtem, přičemž hovor spouštím z počítače, přes který komunikuji se svými studenty a koriguji celou schůzku. Často také sdílím obrazovku a zvuky počítače kvůli videu na YouTube, sdílím nějaké další materiály apod., což pochopitelně jde na počítači mnohem pohodlněji než na iPadu. To ale neznamená, že Zoom na iPadu sdílet neumí. Umí a dobře, jen to prostě není ono a ta odezva, s jakou vaši obrazovku vidí druhá strana, je několikanásobně delší než v případě sdílení obrazovky přes počítač, i když máte upload 40 Mb/s jako já. K čemu ale iPad slouží úplně perfektně, je sdílení Whiteboard neboli tabule. Když nejsem fyzicky schopen lidem něco vysvětlit, tak své myšlenky a poznámky píšu na iPadu, který funguje jako psací plocha pro mé studenty (viz obrázek). Zoom má dokonce integrované funkce Apple Pencil včetně poklepání na střídání tužky a gumy, takže použití je naprosto intuitivní a rychlé, jako byste psali do Wordu nebo Poznámek. Lidé vidí mé poznámky téměř okamžitě a já tak v podstatě nejsem nucen na své hodině či komunikaci s ostatními nic zásadního měnit.

Dovedu si představit výuku bez iPadu, koneckonců ji absolvuji denně na univerzitě, kde učitelé nanejvýš sdílí obrazovku s prezentací a tím to hasne, rozhodně jí ale iPad dá zcela jiný rozměr. Úplně stejně jako na univerzitě to probíhá na škole mojí sestry i ostatních dětí, se kterými jsem se bavil. Žádné poznámky v reálném čase. Skvělé je, že pokud můžete sdílet rukou psané poznámky, jste lidem na druhé straně blíž, všechno je jasnější a jednodušší a oproti fyzickým hodinám se tak kromě toho, že jsme každý doma, nemění skoro nic. Já mám zrovna ve zvyku psát poznámek celkem hodně, takže bych se jako učitel cítil docela svázaný, kdybych je musel v distanční výuce vynechat. Myslím, že díky Zoomu a iPadu jsem svým studentům schopen nabídnout to nejlepší i v těchto ztížených podmínkách, za což jsem vděčný. Jen mě mrzí, že i když na počítači povolím sdílení obrazovky více uživatelům, Zoom mi nedovolí sdílet najednou jak poznámky, tak obrazovku počítače. Občas bych totiž potřeboval sdílet úplně všechno, a musím to řešit jinak. Třeba že sdílím obrazovku počítače, na které vedle sebe otevřu OneNote a další dokumenty, které chci sdílet, a své poznámky píšu do OneNote na iPadu, odkud se přes OneDrive synchronizují v reálném čase do počítače. Je to trochu kostrbatější řešení, ale efekt je nakonec stejný.

S odstupem času uznávám nejen to, že je distanční forma výuky nutná, pokud se lidé nejsou schopni potkat na jednom místě, ale po osobní zkušenosti dokonce vidím výhody, které může učení na dálku přinést. Pokud si člověk dá tu péči a umí s lidmi pracovat, rozdíl mezi výukou přes internet a fyzickými hodinami není až tak propastný, jak jsme si na začátku mysleli. Konkrétně třeba v případě, že musí student na jedinou přednášku dojíždět desítky kilometrů, bych bral jeho distanční účast jako regulérní. Proč by se hodiny nemohly vysílat pro ty studenty a žáky, kteří jsou nemocní nebo z nějakého důvodu nemůžou do školy přijít? Napadá mě v souvislosti s tím, jak si na distanční výuku zvykáme, několik důvodu, proč v budoucnu, až bude po všem, distanční výuku zapojit do běžného školního roku, protože by zásadně přispěla k rozšíření vzdělání mezi širší publikum. Učitelé by měli sloužit vzdělanosti a není důvod, proč by se na zajímavé přednášky nemohli připojovat všichni, kteří o ně mají zájem. Myslím, že jsme na prahu popularizace a zpřístupnění vzdělávání, a budu rád, pokud jsem se nespletl.

Příběhy na pokračování



Magazín ■ Daniel Březina

Luke Skywalker byl mladý farmář na zapadlé písečné planetě, který se shodou okolností zapletl do mezigalaktického konfliktu a pomohl jedné straně k zásadnímu vítězství. Pak obdržel medaili za zásluhy a my diváci dostali ujištění, že příběh se bude dál rozvíjet a pokračovat. A podobně to má i Apple. Jen si zpočátku myslíme, že první díl příběhu je absolutní blbost.

V článku se podíváme na tři příběhy, tři části systému iOS, které zpočátku nedávaly moc smysl a až v dalších verzích systému jsme pochopili, kam tím Apple mířil a jak skvěle to dokázal vymyslet. Takových funkcí a novinek je celá řada a já pro vás vybral tři takové. Každou z jiné oblasti. Softwarovou funkci, hardwarovou funkci a jednu funkci pro vývojáře.

ZBYTEČNÉ POHYBY PRO MLADÉ

Vítejte zpět v roce 2015. Je září a Apple představuje iPhone 6S a 6S Plus. Hlavní novinky? Displej s funkcí 3D Touch a Live Photos. Vrstva pro 3D Touch byla postupně z iPhonu odebrána, ale koncept ovládání zůstal. Ovšem 3D Touch není tou funkcí, která nás zajímá. Nás zajímají rozpohybované Live Photos.

Koncept Live Photos je jednoduchý. Jde o to, že vyfotíte klasickou fotografii, ale systém pro ni natočí krátké video před a po zachycení fotografie. Konkrétně sekundu a půl před a sekundu a půl po zachycení obrázku.

Proč by měl uživatel chtít fotit „oživlé“ fotografie? To je přece jasné, připomenete si tak atmosféru okamžiku. Alespoň podle vyjádření Applu. Po stlačení displeje prstem (u staré 3D Touch vrstvy) si přehrajete celý okamžik. Můžete ho umístit jako tapetu iPhonu a na zamčené obrazovce si ho přehrávat neustále dokola. To zní přece dobře, ne?

Po uvedení této funkce se na Apple snesla kritika, že tohle opravdu iPhone nepotřebuje a že se tím

zbytečně cílí na mladé lidi závislé na Instagramu nebo Snapchatu. Samozřejmě se k tomu přidala tradiční hláška, že Steve Jobs se otáčí v hrobě a Tim Cook Apple ničí. Opak byl ale pravdou. Live Photos započaly éru možností výpočetní fotografie na iPhonu.

iPhone uměl už od verze 4 fotit fotografie v HDR. To znamenalo, že když jsme stiskli spoušť, iPhone vyfotil fotografii a zobrazil ji. Na pozadí ale těch fotografií vyfotil několik a poskládal ideální výsledek. Live Photos ale ukázaly, kam může výpočetní fotografie zajít. Pomocí Live Photos totiž můžete snadno vytvořit dlouhou expozici a bez nutnosti použití přídavných filtrů.

Live Photos je v podstatě zaznamenání pohybu. A iOS dokáže tento pohyb analyzovat a na pozadí s ním pracovat. Chcete mít rozmazanou hladinu tekoucí vody? Světelné čáry od aut na noční dálnici? Ideální pro Live Photos. Ovšem toto jsme se dozvěděli až o pár let později, se softwarovým updatem.

TAJEMNÝ ČIP V IPHONU

To, že nás Apple učí abecedu, víme už dlouho. Máme tu čipy označené písmeny A, W, S, T nebo nově M. A při každém uvedení se jednalo o velkou slávu. Apple se tím chlubil ve všech možných materiálech a stavěl na tom velkou část uvedení produktu. Ovšem existuje jeden čip, jehož potenciál je nám stále skryt, a který nám Apple zatajil. Jedná se o čip řady U.

Čip U1 (ne)byl představen s iPhone 11 a 11 Pro. O jeho existenci jsme se dozvěděli až z technické specifikace. A jeho použití bylo v té době limitováno pouze pro přenos souborů pomocí AirDrop. Fungovalo to tak, že čip poznal, který iPhone je nejblíž, respektive na který iPhone míříme, a upřednostnil ho při přenosu dat. Ruku na srdce, poznali jste někdy rozdíl?

Tajemný čip U1 se dočkal dalších dvou velkých chvil slávy. Jedna přišla na online eventu letos v červnu při příležitosti představení iOS 14. Pomocí iPhonu 11 si nyní můžete odemknout auto, a to právě pomocí U1. Konečně jsme viděli první pořádné využití, i když většina z nás si bude muset počkat několik let na odemykání aut iPhonem. Druhá chvíle slávy přišla na jednom podzimním uvedení novinek, kdy se U1 objevil v HomePodu mini.

V čem je U1 tak speciální a proč nám nestačí klasický Bluetooth? Čip U1 je postaven na technologii Ultra Wide-Band. Tato technologie je velmi úsporná na energii a pro přenos dokáže využít velkou šířku rádiového spektra. Apple ji nazývá jako „GPS pro váš obývák“. A HomePod mini v tom nejspíš sehraje zásadní roli.

Už nyní můžete HomePod mini ovládat pomocí iPhonu. Na iPhonu posloucháte svou oblíbenou hudbu a pak ji pomocí čipu U1 přenesete do HomePodu, který má přehled o poloze jednotlivých zařízení v okolí. Mimo nových iPhonů a HomePodu mini je čip U1 i v nových Apple Watch

Series 6. Jak s tím Apple dál naloží? A proč není U1 i v novem MacBooku s procesorem M1? Příběh bude dále pokračovat.

I VÝVOJÁŘI MAJÍ RÁDI POKRAČOVÁNÍ

Asi nejznámější příběh na pokračování pro vývojáře byl nástroj Auto Layout. Pro nové applisty je možná těžké uvěřit, ale ještě před osmi lety jsme měli pouze jeden iPhone, pouze jednu velikost displeje. Vytvořit uživatelské rozhraní pro jednu velikost displeje bylo velmi jednoduché. Prostě jste jako vývojář řekli, kde přesně má v souřadnicích X a Y prvek UI být. Například jste chtěli mít tlačítko o šířce 100 pixelů a výšce 60 pixelů na pozici X=100 a Y=150. A ať už se aplikace spouštěla na iPhonu 3G, nebo na iPhonu 4, přesně jste věděli, kde tlačítko bude. To se změnilo s příchodem iOS 6.

Operační systém iOS 6 přinesl nástroj Auto Layout. Bavíme se o létě 2012, tedy těsně před zveřejněním iPhonu 5 s novou úhlopříčkou. U Auto Layoutu jste už neudávali přesnou pozici, ale uvedli jste vztah k okolním prvkům UI. Jak daleko má nový element být a na který další prvek UI má být navázaný. Při použití tohoto nástroje jste mohli připravit aplikaci na další rozměry displeje. Pak už bylo jedno, jestli byla změna pouze půl palce jako u iPhonu 5 nebo palec a půl u iPhonu 6 Plus. Mimochodem, v létě před uvedením iPhonů 6 a 6 Plus dal Apple vývojářům možnost zkoušet vzhled aplikace na různých velikostech displeje. Tím jim chtěl naznačit, že může přijít jakákoliv změna. A taky přišla.

ZDRAVÍ NA PRVNÍM MÍSTĚ

Jako bonus tu mám další zajímavý příběh na pokračování, který nejspíš překvapil i samotný Apple. Tím příběhem na pokračování byla knihovna HealthKit s aplikací Zdraví, která přišla s iOS 8. Jednalo se o sběrnici zdravotních dat. Dáno do kontextu, iOS 8 byl představen v červnu 2014. V září 2014 Apple poprvé ukázal světu Apple Watch. A tehdy nejspíš ani v Applu netušili, jak těsný bude vztah mezi aplikací Zdraví a Apple Watch.

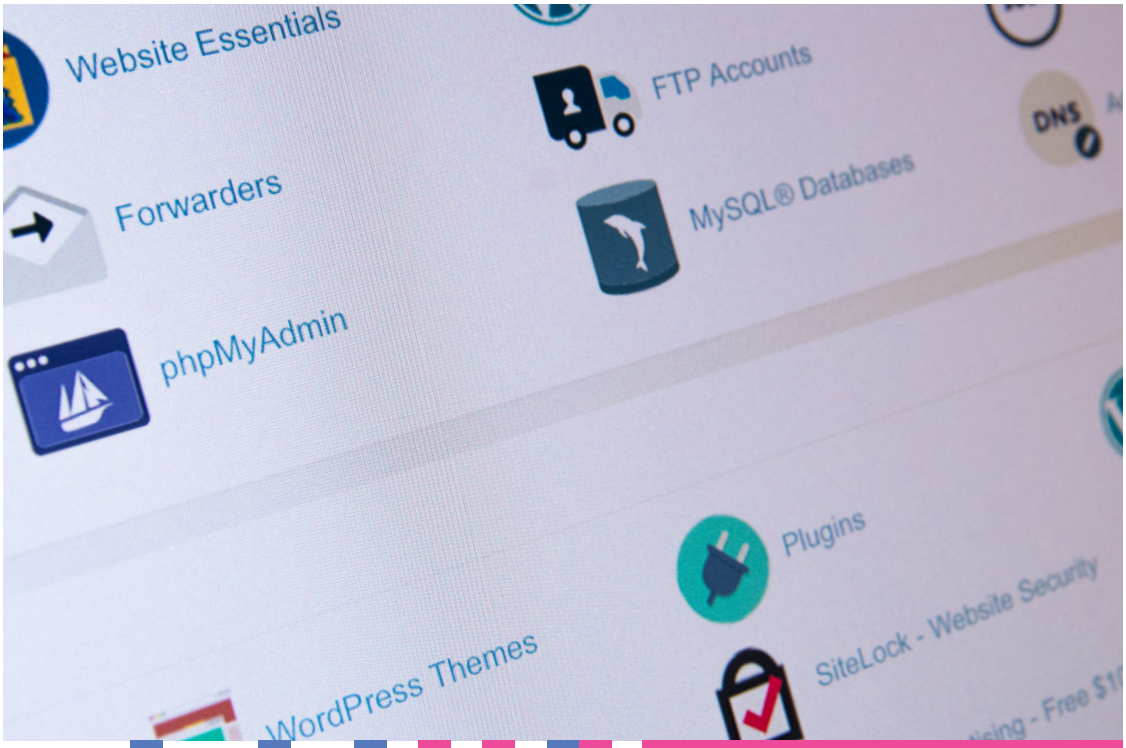
Různé zdravotnické funkce se staly základní funkcionalitou Apple Watch. A vše je poháněno právě vývojářskou knihovnou HealthKit. Tehdy v roce 2014 si vývojáři mysleli, že knihovna HealthKit bude pro pár vyvolených firem, které dodávají vlastní doplňky sledující naše zdraví. Ovšem další rok Apple ukázal sportovní funkce jako měření uběhnuté vzdálenosti nebo měření srdečního tepu. A to otevřelo oči spouště vývojářů.

Apple si v posledních deseti letech, kdy se začal aktivně tvořit jablečný ekosystém, velmi oblíbil příběhy na pokračování. Často nám byla předvedena funkce, kterou jsme nechápali a automaticky jsme ji zavrhovali jako nepoužitelnou. Stačilo ale pár měsíců, jeden nový produkt nebo softwarový update, a vše nám začalo dávat smysl. A to je přesně to, co jsem měl na každé prezentaci nejradši. Když do sebe vše krásně zapadlo. Jaký bude další příběh na pokračování?

Důvěřuj, ale prověřuj!

Magazín ■ Lenka M.

Doby, kdy byla síťová komunikace nešifrovaná, jsou dávno ty tam. V dnešní době je třeba dbát na bezpečnost na každém rohu. Nemůžeme důvěřovat webové stránce jen proto, že vypadá jako stránka banky. Nemůžeme důvěřovat každému e-mailu, který nám přijde do schránky, i když se tváří, jako by byl od úřadu.



Ráda bych proto vás, čtenáře, uvedla do tajů základů kybernetické bezpečnosti. A jedním velmi často skloňovaným pojmem kybernetické bezpečnosti je digitální certifikát. Pojďme se na něj podívat blíže.

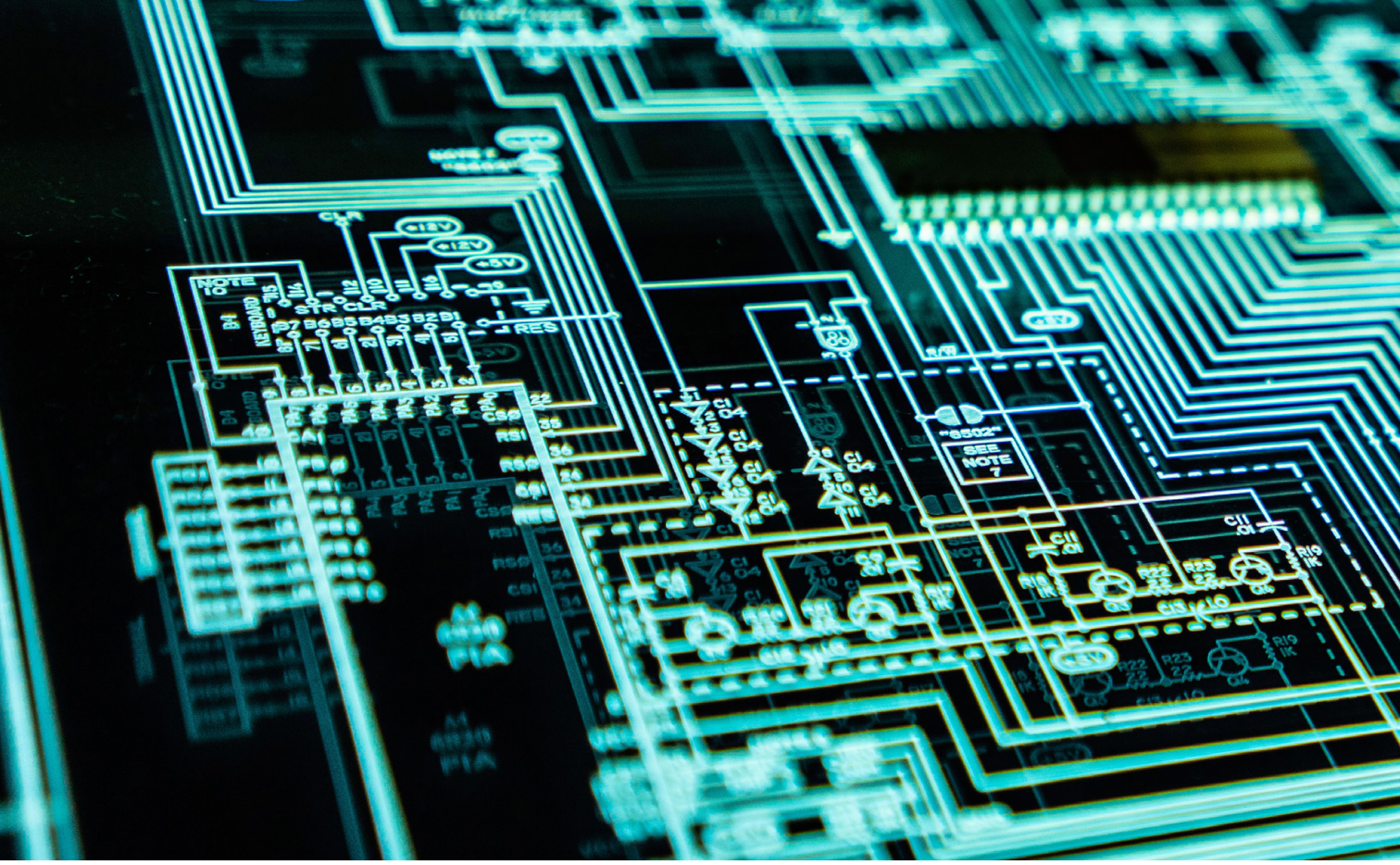
CO JE TO CERTIFIKÁT?

Digitální certifikát je balíček informací, který je vydán a podepsán certifikační autoritou. Tyto certifikáty potvrzují, že daný klíč patří uvedenému vlastníkovi, jako jsou např. webové stránky, organizace či jednotlivci. Digitální certifikáty jsou využívány proto, aby byla zajištěna autentičnost, důvěrnost, nepopiratelnost ze strany odesílatele či příjemce.

Pro začátek je třeba zmínit pojem PKI. Jedná se o infrastrukturu veřejných klíčů, která se stará o vytváření, distribuci, správu či revokování veřejných klíčů. Druhů a úrovní klíčů, kam certifikáty spadají, existuje velké množství. Mezi základní patří osobní komerční certifikát, který slouží k autentizaci uživatele vůči serveru (např. elektronické bankovnictví) či podepisování a šifrování emailů. Tento druh certifikátu ale není uznáván úřady státní správy. Osobní kvalifikovaný certifikát s nejvyšším stupněm důvěryhodnosti slouží k vytváření elektronického podpisu a lze s ním podepisovat dokumenty. Kvalifikovaný certifikát se musí řídit zákonem č. 297/2016 Sb. a je ukládán na USB token nebo čipovou kartu. Serverový certifikát je vydáván pro technická zařízení. Využívají se pro zajištění zabezpečené komunikace se servery či vzájemné komunikace mezi servery. Jako příklad lze uvést zabezpečenou komunikaci klienta s webovým serverem (známý SSL certifikát).

U některých druhů certifikátů různých certifikačních autorit lze narazit i na další dělení dle úrovní, kdy nejnižší úroveň poskytuje nejnižší stupeň důvěryhodnosti a nejvyšší úroveň poskytuje nejvyšší důvěryhodnost. Vždy je třeba vybírat daný certifikát podle toho, k jaké komunikaci bude určen. Pokud bude určen jen pro běžnou e-mailovou komunikaci (s výjimkou úřadů), tak stačí obyčejný osobní komerční certifikát. Pokud je třeba komunikovat s úřady, je třeba využít kvalifikovaného certifikátu. Velmi podobně to funguje u serverových certifikátů SSL. Pokud máte své webové stránky, plně postačí certifikát např. od certifikační autority Let's Encrypt. Pokud se jedná o webové stránky významné organizace, je třeba, aby měla certifikát od nějaké vyšší certifikační autority, čímž získá plnou důvěru.

Velké společnosti mohou využít i hardwarového modulu HSM (Hardware Security Module), což



je fyzické zařízení, které se využívá ke kryptografickým operacím, jako je generování a uchovávání klíčů, vytvoření interní certifikační autority a mnoho dalšího. Má plno bezpečnostních prvků, které znemožňují přístup ke chráněným operacím, a to i v případě krádeže zařízení.

Pro digitální certifikáty je využívána asymetrická kryptografie, což znamená, že se pro šifrování a dešifrování využívají odlišné klíče, a to veřejný a soukromý. Opakem je symetrická kryptografie, kde se využívá k šifrování i dešifrování pouze jediný klíč.

Základní princip nejběžnější verze asymetrické kryptografie je takový, že je veřejný šifrovací klíč volně dostupný a kdokoliv jím může zašifrovat zprávu. Dešifrovací klíč je už ale soukromý a je potřeba, aby byl tajný, neveřejný a pečlivě uschovaný. Tímto klíčem lze zprávy dešifrovat. Oba klíče jsou matematicky svázány, ale není možné se z veřejného klíče dopočítat toho soukromého.

> Veřejný šifrovací klíč je volně dostupný a kdokoliv jím může zašifrovat zprávu. Dešifrovací klíč je soukromý a je potřeba, aby byl tajný a pečlivě uschovaný.

ALICE A BOB

Lze uvést typický příklad, a sice zaslání zprávy Alice Bobovi, kdy Alice vlastní veřejný klíč Boba (který je volně dostupný). Alice zašifruje tímto veřejným klíčem důležitou zprávu, která patří Bobovi a nikdo jiný než Bob si ji nemůže přečíst. Po šifraci Alice pošle zprávu Bobovi a ten, jakožto jediný vlastník soukromého klíče, zprávu dešifruje a může si ji přečíst. Vzhledem k tomu, že nikdo jiný soukromý klíč nevlastní, tak není schopen zprávu dešifrovat. Asymetrické kryptografie je také využíváno pro digitální podpis, kdy pouze majitel tajného klíče může vytvořit podpis a verifikovat jej mohou ti, kteří vlastní veřejný klíč. To je opačný postup než výše uvedený.

Digitální certifikát je uchováván ve formátu X.509. Certifikát obsahuje veřejný klíč X.509, digitální podpis a informace o certifikační autoritě, která jej vydala (verze standardu, sériové číslo, algoritmus, vystavitel, časová platnost, veřejný klíč, podpis apod.). Certifikační autorita (CA) je subjekt, který, jak již bylo výše uvedeno, vydává digitální

certifikáty. Potvrzuje pravost údajů, které se v klíči nacházejí. Certifikační autoritě bychom měli důvěřovat. Je třeba jí důvěřovat, že neudělala v certifikátu chybu, nebo že nebyla ovládána útočníkem. Certifikační autority se snaží, aby jejich důvěryhodnost byla co nejvyšší. Velmi si zakládají na tom, aby jejich důvěryhodnost nebyla jakkoliv narušena. Stačilo by, aby došlo k nějaké mediální masáži konkrétní certifikační autority, a lidé by jí přestali věřit. V minulosti již byly takové případy, že certifikační autorita vydala falešné certifikáty.

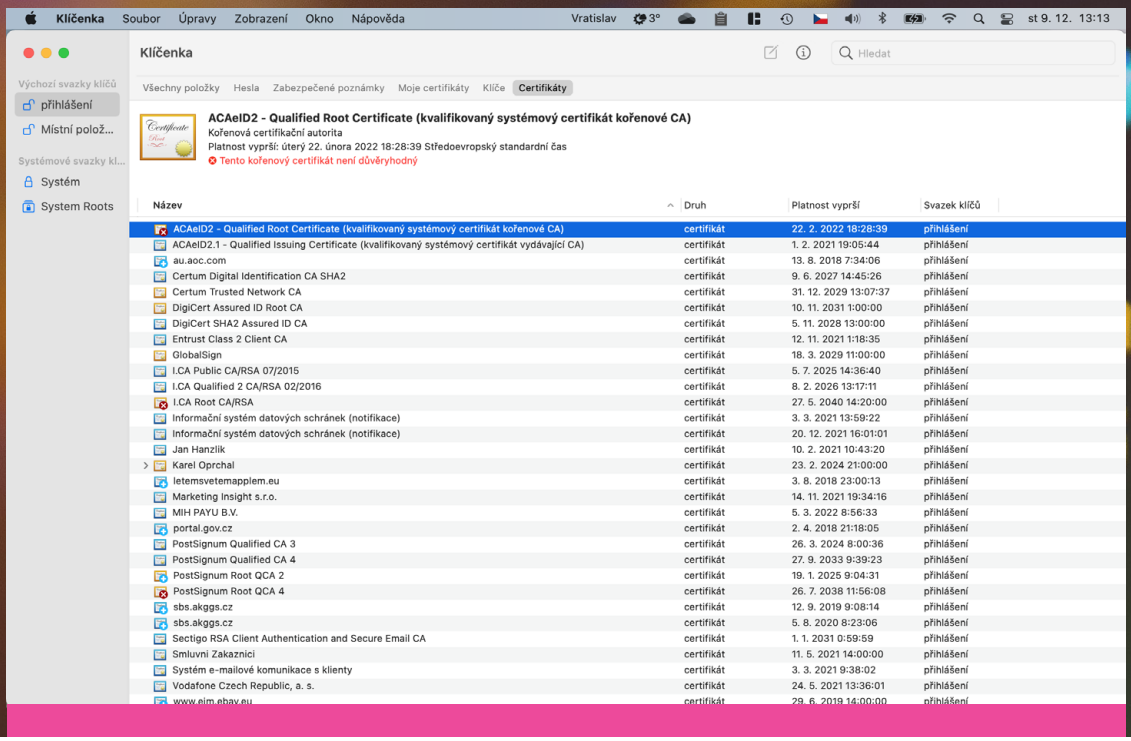
Zde je ještě třeba uvést, že existuje možnost zneplatnění certifikátu – certifikát je tzv. revokován. Důvodem pro zneplatnění je například to, že byl soukromý klíč ztracen, ukraden, okopírován či kompromitován. Seznam revokovaných certifikátů vydává certifikační autorita. Důležité je neplést si expiraci certifikátu (vypršení jeho platnosti), po které již certifikát není platný, s revokací, kdy dojde ke zneplatnění ještě platného certifikátu certifikační autoritou.

Rozhodujícím faktorem je také cena. V podstatě si každý může vydat svůj certifikát, a tím pádem je sám sobě certifikační autoritou, např. pomocí OpenSSL, kde si může kdokoliv vytvořit úplnou osobní certifikační autoritu. Mezi další běžně a hojně využívané certifikáty patří ty od certifikační autority Let's Encrypt, které jsou také zdarma. Každopádně Let's Encrypt vynakládá nemalé finanční prostředky, aby byla důvěryhodná. Za certifikáty od předních certifikačních autorit si ale samozřejmě zaplatíte. Peníze, které se platí za certifikáty, většinou putují na to, aby se vlastní kořenové certifikáty certifikačních autorit rozdistribuovaly do softwarů, které využívají přenosu důvěry, jako jsou operační systémy, webové prohlížeče apod. Mezi největší české poskytovatele certifikačních služeb patří např. První certifikační autorita, a.s., Česká pošta, s.p., a eIdentity a.s.

CERTIFIKÁTY A APPLE

Certifikáty mohou být uloženy buď v operačním systému, nebo na externím médiu (čipová karta, USB token). Některé certifikáty není možné z bezpečnostních důvodů přenést z externího média do operačního systému – lze je použít pouze externě a bývají chráněny pinem.

Pokud se zaměříme na certifikáty v operačním systému, tak každý operační systém disponuje svým interním úložištěm pro certifikáty, kterým bude následně operační systém věřit. Budou jim také důvěřovat prohlížeče či další nainstalovaný software. Certifikáty lze přidat, odstranit, uložit či zobrazit. Úložiště obsahuje také seznam revokovaných



certifikátů. Na zařízeních společnosti Apple je k dispozici celá řada předinstalovaných kořenových certifikátů od různých certifikačních autorit a systémy jako iOS, iPadOS a macOS (případně i watchOS a tvOS) ověřují jejich důvěryhodnost. Pokud se důvěryhodnost nepodaří ověřit, tak je uživatel informován (služba nahlásí problém).

Do iPadOS či iOS lze samozřejmě také ručně doinstalovat další kořenové certifikáty (např. podnikový) a je jen na vás, zda je označíte jako důvěryhodné. Certifikáty lze označovat jako Důvěryhodné, Vždy se dotázat či Blokované. Pokud jsou certifikáty Blokované, zařízení jim nebude důvěřovat. Úložiště důvěryhodných certifikátů najdete v Nastavení – Obecné – Informace a dole najdete Důvěryhodnost certifikátu. Zde najdete i verzi Trust Storu. Na oficiálním webu Apple lze najít přehled předinstalovaných důvěryhodných kořenových certifikátů pro všechny výše uvedené operační systémy. Najdete tam nejen aktuální seznam, ale také archiv pro starší operační systémy.

Systém macOS ukládá certifikáty do zašifrovaného zamčeného kontejneru, kterému se říká svazek klíčů. Ke správě těchto certifikátů, a také svazků klíčů, se používá aplikace Klíčenka. Tato aplikace slouží k ukládání názvů účtů a hesel nejen pro aplikace, ale také např. servery, webové stránky apod. Klíčenka také slouží pro ukládání různých důvěrných informací, jako jsou čísla platebních karet či piny pro bankovní účty. Pokud byste potřebovali některý z veřejných certifikátů zaslat e-mailem někomu jinému, tak v Klíčence zvolte možnost Export. Pokud budete potřebovat certifikát vložit do Klíčenky, zvolte možnost Import, či můžete využít možnosti „přetažení“ certifikátu na ikonu Klíčenky. Certifikáty je možné zobrazit tak, že otevřete Klíčenku a vyberete požadovaný svazek klíčů. Poté kliknete na kategorii Moje certifikáty anebo Certifikáty a zobrazí se certifikáty v daném svazku klíčů. Pokud si přejete získat informace o jednotlivých certifikátech, tak si vyberte konkrétní certifikát dvojklikem a poté v panelu nástrojů klikněte na tlačítko Informace. Pokud byste potřebovali zjistit, zda je certifikát platný, tak je možné využít v Klíčence volby Průvodce certifikací, kde klikněte na Vyhodnotit [název certifikátu]. Zde je třeba vybrat pravidla důvěry (Obecný, E-mailový certifikát, SSL certifikát, Podepsaný certifikát apod.) a kliknete na tlačítko Pokračovat. Operační systém macOS využívá řadu pravidel důvěry k určení důvěryhodnosti certifikátu, takže každý certifikát může obsahovat různé zásady.

Svazek klíčů tedy disponuje certifikáty důvěrných organizací, a pokud např. navštívíte

zabezpečené webové stránky, které jsou opatřeny certifikátem, tak macOS zkontroluje, zda je certifikát důvěryhodný. Pokud není, anebo stránky certifikát nemají, bude uživatel informován. Takto se bude chovat nejen Safari, ale i Chrome či jiný webový prohlížeč, který využívá interní úložiště certifikátů v operačním systému. Pokud bude spojení nedůvěryhodné, prosím, nezadávejte do webové stránky žádné osobní či důvěrné informace, jelikož spojení není šifrované.

GOOGLE CHROME

Pravdou je, že i mezi uživateli Apple je Google Chrome oblíbeným prohlížečem. Jeho vývojáři pomalu připravují novinku, díky níž bude Google Chrome využívat místo úložiště certifikátů v operačním systému úložiště vlastní. Dále již nebude důvěřovat všem certifikátům, kterým důvěřuje operační systém, ale bude důvěřovat jen těm, které bude mít ve svém úložišti. Díky tomu Google získá plnou kontrolu nad důvěryhodnými kořenovými certifikáty. Tato změna se dotkne jak uživatelů macOS, tak Microsoft Windows. Zatím by se neměla dotknout uživatelů Linuxu či ChromeOS.

Myšlenka je to výborná, bohužel problém nastává např. u firemních počítačů, které využívají vlastní certifikační autority (firemní). V tomto případě budou muset správci přidávat certifikát nejen do úložiště v operačním systému, ale také do úložiště Google Chrome.

Vývojáři Google Chrome pomalu připravují novinku, díky níž bude Chrome využívat místo úložiště certifikátů v operačním systému úložiště vlastní.

Na závěr bych si troufla tvrdit, že většina z nás důvěřuje všem certifikátům, které jsou od výrobce uloženy v úložišti certifikátů. Chápu, že není v lidských silách prověřit každý certifikát, který v počítači je, ale je dobré minimálně věnovat pozornost tomu, zda je webová komunikace zabezpečená (komunikace pomocí HTTPS, zámeček v prohlížeči u webové adresy). Je třeba se zaměřit i na to, jak vypadá celá adresa stránky, abyste se nestali obětí nějakého phishingu. Bohužel i phishingová stránka může mít certifikát a komunikace může probíhat pomocí HTTPS. O tom ale zase někdy příště.

NEXT