**Tipy a triky nejlepší pedagožky** >> strana 3

**Vzpomínky na krvavý listopad 1939** >> 5

**Přístroje ovládané myslí už nejsou sci-fi** >> 7

**S bakalářkou mezi světovou špičku** >> 18

Měsíčník Masarykovy univerzity | www.online.muni.cz | listopad 2017

muni

# Informatici našli slabinu v čipech

Zranitelnost na velmi citlivém místě objevili informatici Masarykovy univerzity. Sledovali čipy, které se používají jako ochrana u zvlášť citlivých zařízení a dokumentů, a u výrobků jedné konkrétní firmy přišli na to, že nejsou zdaleka tak bezpečné, jak by měly být.

Členové Laboratoře bezpečnosti a aplikované kryptografie narazili na chybu náhodou. Zkoumali kryptografické klíče generované z velkého množství různých knihoven v čipech, protože je zajímaly jejich vlastnosti. „Přitom jsme zjistili, že způsob, jakým se generují klíče u výrobku německé firmy Infineon Technologies, je problematický. Z veřejné části klíče lze získat jeho tajnou část výrazně rychleji, než by to mělo být možné," přiblížil Petr Švenda, vedoucí výzkumné skupiny.

Vadu u jednoho ze tří největších světových producentů těchto zařízení objevili experti už před několika měsíci, a jak bývá v oboru zvykem, kontaktovali nejdříve výrobce, aby mohl začít pracovat na jejím odstranění. Situace je ale o to komplikovanější, že chyba je v celé produktové řadě a objevila se poprvé už minimálně před deseti lety.

„Nachází se v softwarové knihovně, která generuje klíče a kterou firma používá ve velké části výrobků. Společnost má totiž tuto konkrétní knihovnu certifikovanou a certifikace je drahá," vysvětlil Švenda, proč je zásah široký. Experti vyšli s informací o objevu po dohodě s firmou až po několika měsících a na webu zároveň zveřejnili nástroj, kterým lze chybu detekovat.

Vadné čipy se používají například v dokladech totožnosti, ne však v těch českých, ty obsahují produkty jiného výrobce. Řešit problematickou situaci ale musí Estonci, Španělé nebo Slováci, jejichž občanské průkazy mají právě tato zařízení. Výrobce už v nových produktech chybu napravil a technologické firmy vydaly patřičné aktualizace softwaru.

Všechno ale ještě zcela vyřešeno není. Slovensko kvůli tomu podle informací České tiskové kanceláře začalo dokonce vydávat nové zaručené elektronické podpisy do čipů občanských průkazů. V první vlně o to můžou požádat uživatelé, kteří už podpis použili. Těm, kteří jej nevyužívají, plánují úřady nahrát bezpečnější verzi na dálku v příštích týdnech.

Martina Fojtů

Foto: Petr Nedoma

## V Souboji mistrů padl rekord

Přesně 3826 diváků. Tolik lidí si našlo na konci října cestu do brněnské extraligové DRFG Areny, aby sledovali hokejový duel mezi HC Masaryk University a Univerzitou Karlovou. Zápas hraný v rámci Evropské univerzitní hokejové ligy dostal název Souboj mistrů, protože se střetli domácí akademičtí mistři České republiky a hostující čtyřnásobný vítěz EUHL.

Utkání se stalo v historii ligy rekordním, pokud jde o návštěvnost. Doteď přišlo na některý z jejích zápasů maximálně 1850 fanoušků. Návštěvníci vytvořili skvělou atmosféru i přesto, že výsledkově se domácím utkání příliš nepovedlo a prohráli 3:8. Na extraligovém stadionu se letos hrál první a poslední zápas ligy. Hokejisté HC Muni standardně nastupují v Hokejové hale dětí a mládeže nedaleko parku Lužánky.

>> hcmasarykuniversity.cz

## Brněnský sedmnáctý

Studenti brněnských vysokých škol připravují na 17. listopadu oslavu Mezinárodního dne studentstva. Akce se uskuteční na náměstí Svobody a naváže na ni pietní průvod.

>> brnensky17.cz

## Dvě fakulty volí nové děkany

Akademické senáty přírodovědecké a filozofické fakulty zvolí do konce roku nové děkany. Na přírodovědecké fakulty končí po dvou funkčních obdobích Jaromír Leichmann z ústavu geologických věd. Kandidáti jsou dva, Luděk Bláha z Recetoxu a Tomáš Kašparovský z ústavu biochemie. Vítěz volby, která se uskuteční 20. listopadu, nastoupí do funkce od 1. února příštího roku. Na filozofické fakultě pak končí 31. března první funkční období Milanu Polovi z ústavu pedagogických věd. Návrhy na kandidáty se podávají ještě do 24. listopadu. Volba se odehraje 4. prosince.

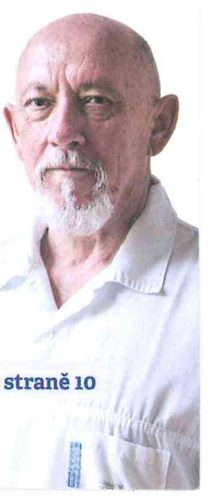
## Zvolte si svého senátora

Volby do Akademického senátu MU pro funkční období 2018 až 2020 se už podruhé v historii odehrají v jednotném termínu ve všech volebních obvodech univerzity. Hlasovat můžou studenti i zaměstnanci, a to od 20. do 24. listopadu v Informačním systému MU. Mezi zásadní pravomoci senátu patří schvalování rozpočtu univerzity nebo i to, že hlasuje o návrhu na jmenování rektora. To bude aktuální v roce 2019, kdy skončí druhé funkční období současného rektora Mikuláše Beka a bude potřeba zvolit jeho nástupce.

>> online.muni.cz/9790

## *Chtěli jsme dát dětem šanci na kvalitní život*

Chirurg Pavel Janíček dotáhl svůj snový projekt a jeho práci ocenila Technologická agentura ČR. Vymyslel rostoucí endoprotézu, díky které už nemusí děti s určitým typem rakoviny kosti stavět před rozhodnutí, jestli amputovat nohu, nebo mít v dospělosti nestejně dlouhé končetiny.



>> čtěte rozhovor na straně 10