# Novinky v oblasti výzkumu a vývoje v kybernetické bezpečnosti

## NÚKIB hledá odborníky na certifikace kybernetické bezpečnosti

Odbor vzdělávání, výzkumu a projektů vypsal výběrové řízení na pozici Specialista EU certifikací kybernetické bezpečnosti. Pokud Vás zajímá tvorba systému evropských certifikací, dohledová činnost a nové technologie a zajímala by Vás práce na NÚKIB tak se neváhejte ozvat! Oceníme také pokud víte o vhodném kandidátovi na tuto pozici a možnost práce na NÚKIB mu zprostředkujete. Celý inzerát na pracovní pozici je dostupný na stránkách NÚKIB.

## Platforma k výzkumu a vývoji v kybernetické a informační bezpečnosti

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) uspořádal 12. listopadu spolu s Vysokým učením technickým v Brně (VUT) v pořadí již druhé setkání Platformy k výzkumu a vývoji v kybernetické a informační bezpečnosti. Platforma, která má v tuto chvíli 22 členů, má za cíl propojit subjekty soukromé, veřejné a akademické sféry, které se zabývají výzkumem a vývojem ve zmíněných oblastech. Více informací naleznete zde.

## Kybernetický polygon MU zvítězil v soutěži Evropské komise Inovační radar

Kybernetický polygon Masarykovy univerzity zvítězil v soutěži Evropské komise Inovační radar. Cena, kterou si za srovnatelný bezpečnostní software účtují komerční subjekty, se běžně pohybuje v řádech milionů korun. Oni ten svůj nabídli zdarma. Více naleznete zde.

## Informační den k výzvám Horizontu Evropa – Digitalizace, průmysl a vesmír

## Bankomaty a strojové učení

Technologické centrum AV ČR pořádá 7. prosince 2021 Národní informační den k výzvám roku 2022 programu Horizontu Evropa, Klastru 4 - Digitalizace, průmysl a vesmír. Cílem odpolední akce je seznámit účastníky s výzvami r. 2022, informovat o novinkách v podávání projektových žádostí, zprostředkovat rady z oblasti hodnocení projektů, sdílet zkušenosti řešitelů a komentovat určité aspekty evropských partnerství, která budou v programu HE implementována. Více o programu zde.

## Publikace *Raising Awareness of Cybersecurity*

ENISA představila zprávu ve které analyzuje politiky a kapacity členských států EU v oblasti jejich schopností zvyšovat povědomí o kybernetické bezpečnosti. Zpráva vedle analýzy stavu v různých zemích poskytuje i přehled jakým způsobem jednotlivé státy začleňují otázku povědomí běžných uživatelů do svých národních kybernetických bezpečnostních strategií. Celá zpráva je k dispozici na webu ENISA.

## Tardigrade malware

(29. 11. 2021; threatpost.com) Výzkumníci z *Bioeconomy Information Sharing and Analysis Center (BIO-SHC)* objevili nový typ malwaru, který pojmenovali *tardigrade* („ževluška“). Za tímto útokem stojí (dle BIO-SHC) nejspíše nejmenované APT skupiny. Nový typ útoku se umí přizpůsobit prostředí ve kterém je nasazen, skrývat se, a dokonce fungovat i autonomně pokud by ztratil spojení s útočníkem. Útok přitom směřoval především na společnosti vyrábějících vakcíny proti onemocnění COVID-19. Malware samotný patří do rodiny tzv. *SmokeLoader*(ů). Ty představují obecnější kategorii backdoor malwarů, které jsou často velmi odlišné od sebe navzájem protože umožňují určitou úroveň modularity. *Tardigrade* útok je na rozdíl od svých předchůdců mnohem propracovanější a mnohem přizpůsobivější.

**Komentář:** Nově objevený typ malwaru se některým výzkumníkům jeví jako nástroj Cobalt Strike. Výzkumníci z BIO-SHC si však stojí za svým názorem, že jde o nový typ malwaru. Sami se přitom nebojí označit jako jeho původce neurčitou APT skupinu. Především se odkazují na to, že malware útočí především na společnosti, které se věnují výrobě vakcín proti COVID-19 což považují za primárně politický zájem.

PETR MARTINEK; p.martinek@nukib.cz
Oddělení výzkumu a evropské spolupráce, NÚKIB