MUNI
ICS

Doporučení pro zajištění kybernetické bezpečnosti v rámci konference ICRI 2022 z pohledu CSIRT-MU

Pro potřeby technické specifikace výběrového řízení realizovaného v rámci mezinárodní konference ICRI 2022, je z pohledu Kyberbezpečnostního týmu Masarykovy univerzity (dále jen „CSIRT-MU“) doporučováno zajištění kybernetické bezpečnosti a bezpečnosti informací v rámci veškerého dodávaného software dle níže definovaných požadavků.

Zajištění informační bezpečnosti

Veškerý dodávaný SW bude z pohledu jednotlivých pořizovaných, zpracovávaných, ukládaných či přenášených informací zajišťovat jejich bezpečnost, a to z pohledu základních tří atributů informační bezpečnosti v podobě CIA triády (C – důvěrnost, I – integrita, A – dostupnost). Minimální úroveň splnitelnosti těchto parametrů je níže definovaná úroveň zajištění bezpečnosti:

- **Dostupnost:** Cílová doba obnovy (tzv. Recovery Time Objective – RTO) se stanovuje na **maximálně 10 minut** v rámci týdne konání konference, tj. 17. - 23. 10. 2022. Mimo tuto dobu se stanovuje na **maximálně 60 minut**.
- **Integrita:** Modifikaci dat se předchází za pomoci využití **bezpečných šifrovacích protokolů a metod využívajících aktuálně odolné kryptografické prostředky** dle doporučení NÚKIB[1].
- **Důvěrnost:** Nesmí dojít k prozrazení dat mimo konferenci ICRI 2022, jelikož se jedná o uzavřený a zvaný event a je tak **nutné zabránit prozrazení dat mimo událost**.

Odůvodnění dostupnosti: Konference běží podle časového plánu, dostupnost je proto time-sensitive a v rámci běhu konference (tedy v horizontu 3 dní) se jedná o zásadní vlastnost systému/služby.

Odůvodnění integrity: Předpokládá se nahrávání konference a následná dostupnost záznamu veřejnosti/zaregistrovaným účastníkům s dopadem závěrů konference na tvorbu politik/širší činnost výzkumných infrastruktur. V rámci běhu konference je tedy schopnost zachovat integritu dat zásadní vlastností systému/služby.

Odůvodnění důvěrnosti: Jedná se o událost pro zvané, registrované či platící účastníky a prozrazení dat mimo událost by tak popřelo její účel (uzavřenost). Pokud mají být data následně dostupná veřejnosti, tak je potřeba pokrýt ochranu osobních údajů registrovaných osob.

[1] https://nukib.cz/download/uredni_deska/Kryptograficke_prostredky_doporuceni_v1.0.pdf

MUNI
ICS

Zajištění bezpečnosti webových a mobilních aplikací

Veškerý dodávaný SW bude poskytovat mechanismy ochrany (detekce i prevence) před kyberbezpečnostními hrozbami v podobě aktuálně platných a relevantních zranitelností definovaných dle metodiky OWASP Top 10 pro webové[2] a mobilní[3] aplikace.

V Brně dne 14. března 2022.

Zpracovali: Bc. Tomáš Plesník (Vedoucí CSIRT-MU)
JUDr. Mgr. Jakub Harašta, Ph.D. (Ústav práva a technologií, PrF MU)

Digitally signed by
Tomáš Plesník
14.03.2022

[2] https://owasp.org/www-project-top-ten/
[3] https://owasp.org/www-project-mobile-top-10/