Kód tématu: 303-IT-CZ

Možnosti penetračního testování v oblasti průmyslových řídících systémů

Školitel: doc. Ing. Bc. Chramcov Bronislav, Ph.D.

Konzultant: Ing. Malaník David, Ph.D., ---

Ústav fakulty: Ústav informatiky a umělé inteligence

Studijní program: Informační technologie

Anotace:

Kybernetické útoky proti IT infrastruktuře vykazují dlouhodobě vzestupný trend a jsou pro společnost i průmyslové podniky kritické. Jedná se o útoky, které jsou pro útočníky velmi lukrativní a v současné době jim poskytují i vysokou míru anonymity. Dále se ukazuje, že zvláště APT útoky jsou schopné překonávat mnoho ochranných prvků. Pokud jsou útočníkem tyto prvky překonány, poskytnou mu mnohdy neomezený přístup do celé infrastruktury sítě. Toto je zvlášť nebezpečné v současnosti, kdy jsou do sítě integrovány prvky Internetu věcí a obecně SMART technologií. Úspěšný útok může způsobit obrovské škody nejen technologické, ale i společenské. Disertační práce je zabývá výzkumem proaktivní bezpečnosti v oblasti průmyslových řídících systémů. Cílem je návrh metodických postupů a pravidel pro aktivní detekci slabých míst pomocí penetračních testů dané infrastruktury. Záměrem práce bude přiblížit problematiku těchto systémů, jenž má zcela jiné priority než systémy informačních technologií a na základě těchto parametrů poté navrhnout postup a pravidla, kterými by se měly subjekty podílející se na testech řídit. Absence metodiky pro takto specifické prostředí ovlivňující kybernetický i fyzický prostor může mít katastrofální dopady. Výzkumné výstupy a navržené postupy budou komparativně hodnoceny s aktuálními metodikami a standarty penetračních testů v oblasti IT. Zároveň bude kladen důraz na specifikaci kritických aspektů a oblastí testování specifických pro průmyslové řídící systémy.

Literatura:

[1] UNAL, Ugur, Ceyda Nur KAHYA, Yaprak KURTLUTEPE a Hasan DAG. Investigation of Cyber Situation Awareness via SIEM tools: a constructive review. _2021 6th International Conference on Computer Science and Engineering (UBMK), Computer Science and Engineering (UBMK), 2021 6th International Conference on_ [online]. 2021, , 676-681 [cit. 2021-11-30]. ISBN 9781665429078. ISSN 25211641. Dostupné z: doi:10.1109/UBMK52708.2021.9558964.

[2] STALLINGS, William a Lawrie BROWN. _Computer security: principles and practice_. Fourth edition. Chennai: Pearson, [2020], 800 atrn. ISBN 978-93-534-3886-9.

[3] KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.

[4] TRAORÉ, Issa, Ahmed AWAD a Isaac WOUNGANG. _Information security practices: emerging threats and perspectives_. Cham, Switzerland: Springer, [2017], 1 online resource. Dostupné z: doi:9783319489476.

[5] ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

[6] MASES, Sten, Kaie MAENNEL, Mascia TOUSSAINT a Veronica ROSA. Success Factors for Designing a Cybersecurity Exercise on the Example of Incident Response. 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS [online]. 2021, , 259-268 [cit. 2021-11-30]. ISBN 9781665410120. ISSN 27680657. Dostupné z: doi:10.1109/EuroSPW54576.2021.00033.

[7] THOMPSON, Eric. Cybersecurity Incident Response. APress, 2018. ISBN 1484238699.