UNIVERZITA J. E. PURKYNĚ V ÚSTÍ NAD LABEM
Přírodovědecká fakulta

Datová a informační bezpečnost

RNDr. Jan Krejčí, Ph.D.

Ústí nad Labem 2020

Předmět: Datová a informační bezpečnost

Studijní program: Aplikovaná informatika

Klíčová slova: Datová bezpečnost, klasifikace a analýza dat, DLP, vysoká dostupnost, zálohování, archivace, logging, framework AAA

Jazyková korektura nebyla provedena, za jazykovou stránku odpovídá autor.

Autor: RNDr. Jan Krejčí, Ph.D.

Obsah

Úvodní slovo

Předmět je koncipován jako pokročilý kurz v oblasti datové a informační bezpečnosti v reflexi na aktuální trendy a potřeby v oblasti kybernetické bezpečnosti.

Způsob ukončení předmětu je zápočtem. Zápočet je rozdělen do dvou částí: laboratorní projekt a písemný test. Za laboratorní projekt je možno získat až 75 bodů, za písemný test 25 bodů. Úspěšný jsou studenti, kteří v součtu získají minimálně 75 bodů.

Příklad písemného testu

Maximální počet bodů za správně vypracovanou otázku je uveden v závorce. Minimální úspěšnost je 75 %.

1. Která data jsou tzv. citlivá? (1)
2. Jaké problémy řeší technologie pro DLP? (1)
3. Pomocí jaké vlastnosti logů dochází k párování systémových logů? (1)
4. Jakou technologii je vhodné využít pro zajištění více četných archivů? (1)
5. Jaká je odolnost pole RAID 1, RAID 5 a RAID 60? (1)
6. Jak mají být data archivována v závislosti na jejich citlivosti? (1)
7. Co je distribuované úložiště? (1)
8. Co je RPO a RTO? (1)

1 Úvod do datové bezpečnosti

CÍLE KAPITOLY

Náplň látky této kapitoly je popsána v literatuře [2].

KLÍČOVA SLOVA

data, bezpečnost, směrnice, nařízení

SHRNUTÍ

Jedná se o úvodní kapitolu, ve které bude řešena základní terminologie. V této kapitole se tedy seznámíte s terminologií a základními definicemi v rámci řízení bezpečnosti dat.

OTÁZKY

1. Co jsou to data?
2. Jaké jsou specifické aspekty korporátních/firemních dat?
3. Která data jsou tzv. citlivá?

OTÁZKY K ZAMYŠLENÍ

1. Jaké jsou základní kameny ochrany firemních dat?
2. Jakým způsobem se data rozdělují?

ÚKOLY

1. Definujte a charakterizujte vzorové příklady dat.

MÍSTO PRO VAŠE POZNÁMKY

2 Datová klasifikace a analýza dat

CÍLE KAPITOLY

Náplň látky této kapitoly je popsána v literatuře [3].

KLÍČOVA SLOVA

kategorizace dat, analýza dat

SHRNUTÍ

Po prostudování byste měli být schopni analyzovat firemní data.

OTÁZKY

1. Co jsou to data?
2. Jaké jsou specifické aspekty korporátních/firemních dat?
3. Co je to DLP?

OTÁZKY K ZAMYŠLENÍ

1. Jaké technologie pomohou řešit DLP?
2. Která data jsou tzv. citlivá?
3. Jakým způsobem se data rozdělují?

ÚKOLY

1. Nalezněte a otestujte volně použitelnou technologii pro DLP.

MÍSTO PRO VAŠE POZNÁMKY

3 DLP systémy

CÍLE KAPITOLY

Náplň látky této kapitoly je popsána v literatuře [2, 4, 5, 6].

KLÍČOVA SLOVA

životní cyklus, vznik, zálohování, archivace, likvidace

SHRNUTÍ

Po prostudování byste měli být schopni, implementovat základní DLP a definovat její politiky.

OTÁZKY

1. Co je to DLP?
2. Jak vznikají bezpečnostní politiky pro zacházení s daty?
3. Kde bývá definována zodpovědná osoba za řízení rizik v rámci nakládání s firemními daty?

OTÁZKY K ZAMYŠLENÍ

1. Jaké problémy řeší technologie pro DLP?
2. Jak části obsahuje pojem DLP?

ÚKOLY

1. Nalezněte a otestujte volně použitelnou technologii pro DLP.

MÍSTO PRO VAŠE POZNÁMKY

4 Systémy vysoké dostupnosti datových úložišť

CÍLE KAPITOLY

Náplň látky této kapitoly je popsána v literatuře [7, 8, 9, 10].

KLÍČOVA SLOVA

RAID, pole, diskové systémy, LUN, Volume

SHRNUTÍ

Obsah probíraného učiva směřuje ke kompetenci rozpoznat vlastnosti datových úložišť.

OTÁZKY

1. Co jsou to pole RAID?
2. Jakou výhodu zajišťuje řešení diskových LUN v rámci dedikovaných polí?
3. Za jakých okolností volíme SAS vs. iSCSI konektivitu polí?

OTÁZKY K ZAMYŠLENÍ

1. Jaké výhody má diskové pole RAID 6 oproti RAID 5?
2. Jaká je odolnost pole RAID 1, RAID 5 a RAID 60?

ÚKOLY

1. V rámci virtualizace implementujte některou volně dostupnou NAS technologií a nad ní definujte LUN z připojených diskových úložišť.

MÍSTO PRO VAŠE POZNÁMKY

5 Zálohovací technologie pro koncové prvky

CÍLE KAPITOLY

Náplň látky této kapitoly je popsána v literatuře [11, 12].

KLÍČOVA SLOVA

koncový prvek, zálohování, technologie, úložiště

SHRNUTÍ

Po prostudování byste měli být schopni zhodnotit zálohovací komerční i nekomerční zálohovací platformy koncových prvků.

OTÁZKY

1. Jakou technologii je vhodné nasadit pro zálohování osobních dat koncového uživatele?
2. Co je RPO a RTO?

OTÁZKY K ZAMYŠLENÍ

1. Jaké aspekty má zálohování osobních dat?
2. Jaké vlastnosti dat je nezbytné analyzovat před volbou zálohovacích či archivačních technologií?

ÚKOLY

1. Využijte online free dostupnou technologii pro zajištění zálohování uživatelských dat.

MÍSTO PRO VAŠE POZNÁMKY

6 Zálohovací technologie pro infrastrukturní systémy

CÍLE KAPITOLY

Náplň látky této kapitoly je popsána v literatuře [13, 14].

KLÍČOVA SLOVA

zálohování, přírůstkové, rozdílové, deduplikace, replikace

SHRNUTÍ

Obsah kapitoly je zaměřen na problematiku metod zálohování infrastrukturních systémů od virtualizačních platforem k duplikacím diskových úložišť.

OTÁZKY

1. Jakou technologií zvolit pro zálohování serverových sdílených úložišť?
2. Jakou technologii použít pro řešení odolnosti virtualizačních platforem?
3. Co je distribuované úložiště?

OTÁZKY K ZAMYŠLENÍ

1. Jaké technologie a protokoly využijete v rámci distribuovaných úložišť?
2. Co je deduplikace dat?
3. Co je replikace dat?

ÚKOLY

1. Díky online dostupných free aplikacím vytvořte distribuované úložiště.

MÍSTO PRO VAŠE POZNÁMKY

7 Archivační technologie

CÍLE KAPITOLY

Náplň látky této kapitoly je popsána v literatuře [15, 16, 17].

KLÍČOVA SLOVA

archivace, likvidace/skartace dat

SHRNUTÍ

Kapitola pojednává o způsobech archivace dat, dle jejich citlivosti.

OTÁZKY

1. Co je archivace dat?
2. Jak mají být data archivována v závislosti na jejich citlivosti?
3. Jak se liší archivace osobních a firemních dat?

OTÁZKY K ZAMYŠLENÍ

1. Co jsou komprimační algoritmy a kdy se využívají?
2. Jakou technologii je vhodné využít pro zajištění více četných archivů a proč?

ÚKOLY

1. Otestujte volně dostupnou aplikaci umožňující řešení přírůstkových a rozdílových archivů.

MÍSTO PRO VAŠE POZNÁMKY

8 Systémy logování a struktura logů pro framework AAA

CÍLE KAPITOLY

Náplň látky této kapitoly je popsána v literatuře [20, 21].

KLÍČOVA SLOVA

AAA framework, systémové logy, analýza logů

SHRNUTÍ

Po prostudování byste měli být schopni definovat, co je systémový log a jaké má základní údaje, popsat, proč je nezbytné tyto informace uchovávat a jak s nimi pracovat.

OTÁZKY

1. Jak jsou strukturované logy?
2. Jaké vlastnosti sledovaných systémů je nezbytné synchronizovat?
3. Pomocí jaké vlastnosti logů dochází k jejich párování?

OTÁZKY K ZAMYŠLENÍ

1. Bez kterého údaje nejsme schopni provést analýzu posloupnosti systémových informací?
2. Co je parsování?
3. Jaké technologie se dají pro ukládání systémových informací využít?
4. Proč je nutné ukládat systémové logy na dedikovaném systému?

MÍSTO PRO VAŠE POZNÁMKY

9 Správa systémů pro ukládání logovacích údajů frameworku AAA

CÍLE KAPITOLY

Problematika vychází z dříve nabytých vědomostí a jedná se praktická cvičení.

SHRNUTÍ

Praktická úloha pro implementaci a správu systémů infrastrukturních logů.

ÚKOLY

1. Využijte volně dostupný systém pro sledování systémových logů a implementujte jej minimálně na 3 koncové systémy.

MÍSTO PRO VAŠE POZNÁMKY

10 Vyhledávání souvislostí v uložených datech

CÍLE KAPITOLY

Problematika vychází z dříve nabytých vědomostí a jedná se praktická cvičení.

SHRNUTÍ

Po absolvování budou frekventanti schopni realizovat tzv. „troubleshooting“ v rámci logovacích informací systémových služeb.

ÚKOLY

1. Analyzujte dostupné systémové logy a vyhledejte v nich, kdy došlo k prvnímu bezpečnostnímu incidentu.

MÍSTO PRO VAŠE POZNÁMKY

Literatura

[1] **DOSEDĚL, T.**: *Počítačová bezpečnost a ochrana dat*, Brno: Computer Press, 2004. ISBN 8025101061.

[2] Broschinski, P. (2017). Zabezpečení firemní infrastruktury proti úniku dat Dostupné z: https://digilib.k.utb.cz/bitstream/handle/10563/40886/broschinski_2017_dp.pdf?sequence=1&isAllowed=y

[3] HOLČÍK, J.. Analýza a klasifikace dat. 2012. [cit. 1.2.2020]. Dostupné z: https://www.iba.muni.cz/res/file/ucebnice/holcik-analyza-klasifikace-dat.pdf

[4] CSTL (2017). A Beginners Guide to DLP:The What, the Why and the HowA Beginners Guide to DLP: The What, the Why and the Hos. Dostupné z: https://www.cstl.com/Clearswift/Adaptive-Redaction/Clearswift_DLP_White_Paper_Web_Ready.pdf

[5] Nikitinsky, N. & Sokolova, T. & Pshehotskaya, E. (2014). DLP Technologies: Challenges and Future Directions. Dostupné z: https://www.researchgate.net/publication/268462340_DLP_Technologies_Challenges_and_Future_Directions

[6] CLOUD SECURITY ALLIANC (2012). SecaaS Implementation Guidance, Category 2: Data Loss Prevention. Dostupné z: https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_2_DLP_Implementation_Guidance.pdf

[7] Andrian, Yoga & Kim, & Ju,. (2019). A Distributed File-Based Storage System for Improving High Availability of Space Weather Data. Applied Sciences. 9. 5024. 10.3390/app9235024. Dostupné z: https://www.researchgate.net/publication/337450101_A_Distributed_File-Based_Storage_System_for_Improving_High_Availability_of_Space_Weather_Data

[8] VERITAS. (2019). Storage Foundation Cluster File System High Availability 7.4 Administrator's Guide-Linux. Dostupné z: https://www.veritas.com/bin/support/docRepoServlet?bookId=133045699-133045726-1&requestType=pdf

[9] DELL Inc. (2020). High Availability and Data Protection with Dell EMC PowerScaleNAS. Dostupné z: https://www.dellemc.com/en-me/collaterals/unauth/white-papers/products/storage/h10588-isilon-data-availability-protection-wp.pdf

[10] Intel Corporation (2014). Architecting a High Performance Storage System. Dostupné z: https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/architecting-a-high-performance-storage-system-white-paper.pdf

[11] Gartner (2016). Use These Five Backup and Recovery BestPractices to Protect Against Ransomware. Dostupné z: http://www.measurecontrol.com/wp-content/uploads/2017/05/gartner-seguridad-en-la-nube.pdf

[12] PARABLU (2017). SMB Guide for Secure Cloud Backup of Endpoints. Dostupné z: https://www.parablu.com/wp-content/uploads/2017/02/SMB-Guide-for-Cloud-Endpoint-Backup-Parablu_old_may2017.pdf

[13] Hewlett-Package Development Company (2015). What You Need To Know Now For Modern Backup. Dostupné z: https://www.parablu.com/wp-content/uploads/2017/02/SMB-Guide-for-Cloud-Endpoint-Backup-Parablu_old_may2017.pdf

[14] DELL Inc. (2012). WHITE PAPER: Backup and Recovery Changes Drive IT Infrastructure and Business Transformation. Dostupné z: https://www.delltechnologies.com/content/dam/digitalassets/active/en/unauth/white-papers/ar-backup-and-recovery-changes-drive-it.pdf

[15] Informatica. (2019). Informatica Data Archive. Dostupné z: https://www.informatica.com/content/dam/informatica-com/en/collateral/data-sheet/data-archive_data-sheet_6955.pdf

[16] Janée, G., Mathena, J., Frew, J. (2008). A Data Model and Architecture for Long-term Preservation. Dostupné z: http://www.ngda.org/research/Tech%20Arch/jcdl-paper.pdf

[17] Turner, S.M., (2001). Guidelines for DevelopingITS Data Archiving Systems. Dostupné z: https://static.tti.tamu.edu/tti.tamu.edu/documents/2127-3.pdf

[18] **SANTUKA, V.**: *AAA identity management security*, Indianapolis, IN: Cisco Press, c2011. ISBN 9781587141447.

[19] **ERICKSON, J.**: *Hacking: the art of exploitation*. 2nd ed. San Francisco, CA: No Starch Press, c2008. ISBN 9781593271442.

[20] Hofstede, R., Čeleda, P., Trammell, B., Drago, I., Sadre, R., Sperotto, A. and Pras, A., (2014).Flow Monitoring Explained:From Packet Capture to Data Analysis withNetFlow and IPFIX. Dostupné z: https://is.muni.cz/publication/1181098/flow-monitoring-explained-paper.pdf

[21] Belfo, F. & Trigo, A. (2013). Accounting Information Systems: Tradition and Future Directions. Procedia Technology. 9. 536-546. 10.1016/j.protcy.2013.12.060.