10.11 Řízení technických zranitelností

Tento dokument popisuje opatření, které MUSÍ nebo BY MĚLO být implementováno pro:

- **Řízení technických zranitelností hardwaru (HW), softwaru (SW) a systémů ICT)**
- **Stanovení pravidel omezení instalace SW vybavení.**
- **Stanovení pravidel a postupů vyhledávání opravných SW balíčků.**
- **Stanovení pravidel a postupů testování oprav programového vybavení.**
- **Stanovení pravidel a postupů nasazení oprav programového vybavení.**

Tento dokument je vyhotoven v souladu s Vyhláškou o kybernetické bezpečnosti. Řízení provozu a komunikací (§ 10).

---

1 Principy (obecné) řízení technických zranitelností

Cíl: Zajistit procesy odhalování zranitelných míst v produktech a službách a následně zajistit postupy zacházení se zranitelnostmi dle doporučení „identifikace-vyhodnocení-zvládání-kontrola“.

1.1 Odhalování zranitelností

Společnost MUSÍ stanovit pravidla pro odhalování zranitelností.

Implementační pokyny:

1.1.1 Společnost MUSÍ přijímat zprávy o potenciálních zranitelnostech.

- Za sledování zpráv o zranitelnostech je odpovědný CISO/manažer kybernetické bezpečnosti (MKB)

1.1.2 Společnost MUSÍ zveřejňovat informace o nápravě zranitelností.

- Za zveřejňování zpráv o zranitelnostech je odpovědný MKB?
- Standardní postupy techniky a zásady týkajících se zveřejnění zranitelností jsou doporučeny viz bod 1.3.

1.2 Postupy zacházení se zranitelnostmi

MUSÍ být nastaveny adekvátní postupy zacházení se zranitelnostmi.

Implementační pokyny:

1.2.1 Za stanovení postupu zacházení se zranitelnostmi je odpovědný MKB

1.2.2 Zpráva o zranitelnosti MUSÍ být ověřena

1.2.3 Do aktivit při řešení zranitelnosti BY MĚL být zapojen pověřený tým

1.3 Nejlepší praktické postupy

Společnost BY MĚLA využívat doporučené nejlepší praktické postupy při realizaci bezpečnostních opatření pro řešení zranitelnosti.

Implementační pokyny:

1.3.1 Zdroje zranitelností

- Common Vulnerabilities and Exposure – **CVE**
  https://cve.mitre.org/cve/
  https://cvetrends.com
- CERT/CC Vulnerability Notes Database – **VU**
  https://www.kb.cert.org/vuls/
- CISA Vulnerability Catalog – **ICS-ALERT, ICSA**
  https://www.cisa.gov/uscert/ics

2 Pravidla pro omezení instalace programového vybavení

Společnost MUSÍ důsledně dbát, aby byl instalovaný software (SW) v souladu s autorským zákonem.

Implementační pokyny:

2.1.1 Společnost MUSÍ zabezpečit oprávněnost instalace a používání SW vybavení.
2.1.2 Společnost MUSÍ zajistit řádnou registraci SW vybavení.
2.1.3 Společnost MUSÍ vést evidenci licencí SW vybavení.
2.1.4 Společnost MUSÍ vést evidenci o instalaci SW vybavení.
2.1.5 Společnost MUSÍ vést evidenci o vyřazení SW vybavení.

3 Pravidla a postupy opravných programových balíčků

Společnost MUSÍ zabezpečit nasazení řízení oprav SW vybavení (záplatování, Patch management). Společnost MUSÍ stanovit pravidla pro vyhledávání, testování a nasazení oprav SW vybavení.

3.1 Vyhledávání oprav programového vybavení

Implementační pokyny:

3.1.1 Postupy při vyhledávání oprav SW vybavení se MUSÍ řídit pravidly poskytovatele oprav a MUSÍ být zdokumentovány.
3.1.2 Provozní postupy a zdokumentované postupy pro změny v systémech BY MĚLY podléhat formální správě dokumentů a změny BY MĚLY být schváleny zodpovědným vedoucím.

3.2 Testování oprav programového vybavení

Implementační pokyny:

3.2.1 Postupy pro testování oprav SW vybavení po implementování opravných balíčků se MUSÍ řídit pravidly pro testování opraveného SW vybavení (NESMÍ být ovlivněn rutinní provoz společnosti) a MUSÍ být zdokumentovány.

3.2.2 Provozní postupy a zdokumentované postupy pro změny v systémech BY MĚLY podléhat formální správě dokumentů a změny BY MĚLY být schváleny zodpovědným vedoucím.

3.3 Nasazení oprav programového vybavení

Implementační pokyny:

3.3.1 Postupy pro nasazení oprav SW vybavení MUSÍ být v souladu s bezpečností a kontinuitou rutinního provozu a MUSÍ být zdokumentovány.

3.3.2 Provozní postupy a zdokumentované postupy pro změny v systémech BY MĚLY podléhat formální správě dokumentů a změny BY MĚLY být schváleny zodpovědným vedoucím.

Použité zdroje

(1) ČESKÁ REPUBLIKA. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti. In: *Sbírka zákonů*. 2018, Ročník 2018, Částka 43, č. 82. Dostupné také z: https://www.psp.cz/sqw/sbirka.sqw?cz=82&r=2018

(2) *MINIMÁLNÍ BEZPEČNOSTNÍ STANDARD* [online]. Verze 1.0. NÚKIB, 2020 [cit. 2022-04-20]. Dostupné z: https://archi.gov.cz/_media/dokumenty:2020-07-17_minimalni-bezpecnostni-standard_v1.0.pdf

(3) *ČSN EN ISO/IEC 27002 (369798) Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací. Technická normalizační komise, 2014.*

(4) *ČSN P 73 4450-1 (734450) Fyzická ochrana prvku kritické infrastruktury - Část 1: Obecné požadavky. CTN Česká asociace bezpečnostních manažerů, 2013.*

Příloha A: Interpretace klíčových slov

Klíčové slovo	Interpretace
MUSÍ	Naprostý požadavek (**bez výjimek**).
NESMÍ	Naprostý zákaz (**bez výjimek**).
MĚLY BY	Doporučený požadavek, mohou existovat platné důvody pro částečné nebo úplné odchýlení od uvedeného, ale MUSÍ být pochopeny a pečlivě zváženy plné důsledky takového chování dříve, než dojde k volbě odlišného postupu (**výjimky jsou možné po zhodnocení rizik a přijetí zbytkových rizik**).
NEMĚLO BY	Doporučený zákaz, záporná forma MĚLO BY (**výjimky jsou možné po zhodnocení rizik a přijetí zbytkových rizik**).
MŮŽE	Plně volitelné (není sledováno v rámci monitorování shody)