

Vybraná kybernetická rizika a jejich předcházení

Radek Zajíc

zajicra1@cvut.cz

Masarykův ústav vyšších studií, České vysoké učení technické v Praze, Česká republika

Úvod

Organizace ve dnešním světě zpracovávají a uchovávají čím dál více svých aktiv v digitální podobě. Každá organizace, od nejmenších po ty největší, by měla analyzovat kybernetická rizika, která jí hrozí, a přijmout opatření pro jejich minimalizaci.

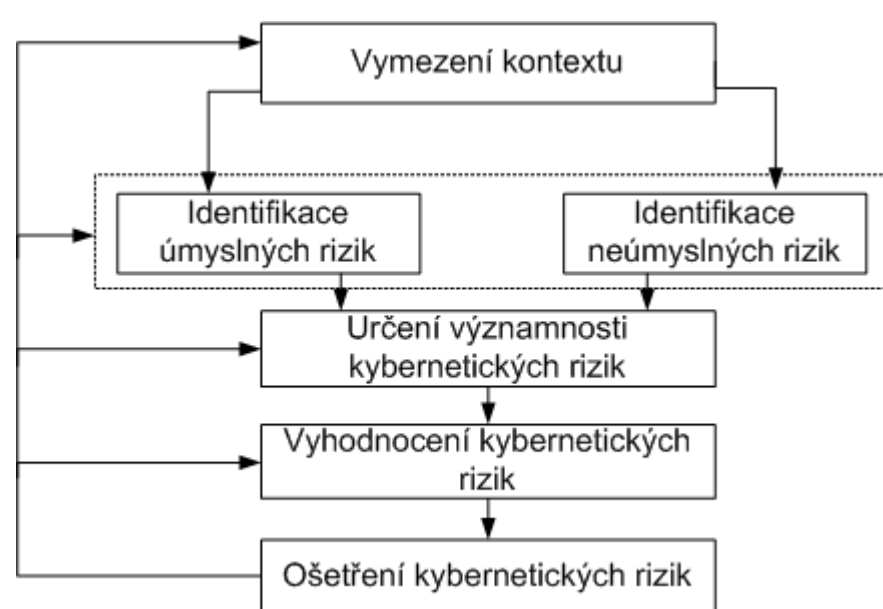
Cíle

Práce popisuje řízení kybernetických rizik, analyzuje a popisuje je. Vysvětluje možné příčiny. Poskytuje přehled nejčastěji se vyskytujících kybernetických rizik, incidentů či hrozeb. Navrhuje opatření pro minimalizaci uvedených rizik.

Metody

Mezi základní části procesu hodnocení rizik patří vymezení kontextu, ve kterém rizika řídíme, identifikace přítomných rizik, určení významnosti rizik, vyhodnocení rizik, ošetření rizik a monitorování a prověřování systému řízení rizik.

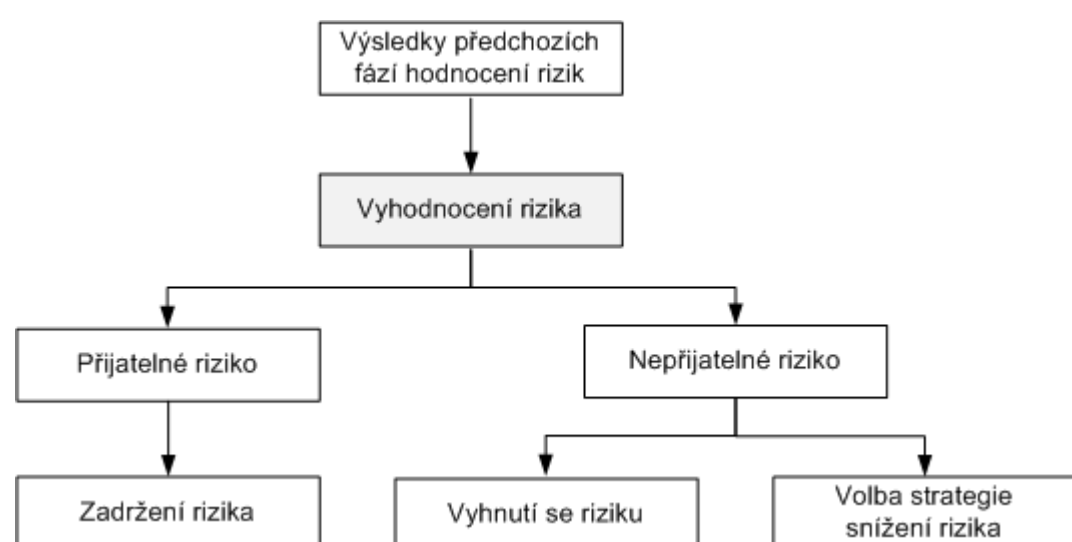
Proces hodnocení kybernetických rizik



Obrázek 1 - Proces hodnocení rizik

Čtenář se seznámí i s procesem rozhodování o riziku.

Proces rozhodování o riziku



Obrázek 2 - Proces rozhodování o riziku

Identifikované hrozby

Bezodůvodné smazání dat	Nesprávný vývoj Chyby v aplikacích
Chyby v aplikacích	Odposlech dat
Infiltrace sítě	Počítačové viry v organizaci
Krádež dat	Průnik do sítě
Krádež zařízení	Předčasné ukončení podpory
Neautorizovaný přístup	Přetížení aplikace
Nedostatečná redundance	Přetížení datové infrastruktury
Nedostatečné nastavení oprávnění	Přetížení systému
Neexistující nebo nefunkční plán pro zotavení z katastrofické události	Selhání úložiště
Neexistující šifrování	Společné uživatelské a technologické sítě
Neexistující, netestované nebo nefunkční zálohování	Špatná péče o kybernetické prostředí
Nenastavená autentizace	Zcizení autentizačních údajů
Neoprávněná publikace dat	Ztráta konektivity
Neřízený zaměstnanec	Ztráta přístupu k datům, které má pod svou správou zaměstnanec (cloud computing)

Shrnutí

Proti kybernetickým rizikům lze úspěšně bojovat. Volbou vhodných opatření lze rizika ošetřit a úplně je eliminovat, nebo alespoň snížit pravděpodobnost výskytu nebo jejich dopad. Práce některá opatření nabízí, oblast kybernetických rizik je nicméně stále nedostatečně probádaná a poskytuje prostor k výzkumu jak v ekonomicko-manažerských vědách, tak ve vědách technických.

Literatura

- VEBER, Jaromír. Management. ISBN 978-80-7261-200-0.
KRULIŠ, Jiří. Jak vítězit nad riziky. ISBN 978-80-7201-835-2.
TRIM, Peter R et al. Cyber security management. ISBN 978-1-472432094.
REFSDAL, Atle et al. Cyber-Risk Management. ISBN 978-3-319-23569-1.
BOEHM, Barry. Software risk management. ISBN 0-8186-8906-4.
SMEJKAL, Vladimír et al. Řízení rizik ve firmách a jiných organizacích. ISBN 978-80-247-3051-6.