

BEZPEČNOST KYBERPROSTORU
25.10.2011

STRATEGIE PRO OBLAST KYBERNETICKÉ BEZPEČNOSTI
ČESKÉ REPUBLIKY NA OBDOBÍ 2011 - 2015

Proč potřebujeme strategii ?

Z čeho vzešla ?

Východiska

ICT významně ovlivňuje fungování vyspělé společnosti a ekonomiky

ICT a společnosti na nich závislé jsou zranitelné

Základní principy

Problematiku kybernetické bezpečnosti nelze vnímat jako izolovaný problém

Propojení a posílení spolupráce všech sektorů společnosti

Vzájemná důvěra a sdílení informací

Individuální zodpovědnost

schopnost přijímat vhodná opatření pro zajištění bezpečnosti a spolehlivosti vlastních ICT systémů a sítí.

Odpovědnost podnikatelského sektoru

definovat minimální standardy kybernetické bezpečnosti a vyžadovat jejich zavedení do praxe a jejich důsledné dodržování.

Základní principy

Resortní spolupráce
MKRPKB

Mezinárodní spolupráce
v oblasti kybernetické a informační bezpečnosti zejména v rámci NATO a EU

Přiměřenost přijatých opatření
ochrana soukromí, základní lidská práva, svobodný přístup k informacím a další demokratické principy. Přiměřenost přijatých opatření

Strategické cíle a opatření

Vytvoření legislativního rámce

vymezení činnosti příslušného orgánu při koordinaci postupu veřejné moci v oblasti kybernetické bezpečnosti, povinnosti pro subjekty vytvářející či využívající ICT služby, a také vymezení formy (způsoby) a rámce (rozsahy) spolupráce se soukromým sektorem a s veřejností.

Posilování kybernetické bezpečnosti v ICT veřejné správy a KI

Zavádění bezpečnostních norem v informačních systémech veřejné správy a prvcích KI

Vybudování vládního pracoviště CERT

zajištění bezpečnosti a spolehlivosti informačních a komunikačních systémů zapojených do KI pomocí vládního koordinačního místa

Strategické cíle a opatření

Mezinárodní spolupráce

Koordinovaná mezinárodní spolupráce

Spolupráce státu, soukromé a akademické sféry

neustálá spolupráce

Zvyšování povědomí o kybernetické bezpečnosti

Nedostatečná informovanost o zabezpečení ICT systémů představuje vážná rizika.