- Legislativní rámec České republiky pro oblast kybernetické bezpečnosti je založen na několika zákonech a předpisech, které mají za cíl ochranu kybernetického prostoru, prevenci kybernetických hrozeb a řízení kybernetických incidentů.

Mezi hlavní legislativní dokumenty patří:

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti - tento zákon stanovuje základní pravidla pro kybernetickou bezpečnost v České republice, včetně povinností pro subjekty kritické infrastruktury, požadavků na bezpečnostní opatření a postupy při kybernetických incidentech.
- Nařízení vlády č. 302/2016 Sb., o kybernetické bezpečnosti - toto nařízení upravuje detailnější technické a organizační požadavky na kybernetickou bezpečnost pro subjekty kritické infrastruktury, včetně pravidel pro hodnocení a hodnocení stavu kybernetické bezpečnosti.
- Nařízení vlády č. 317/2016 Sb., o národním středisku kybernetické bezpečnosti - toto nařízení zakládá Národní středisko kybernetické bezpečnosti (NÚKIB) jako hlavní instituci odpovědnou za koordinaci kybernetické bezpečnosti v České republice.
- Vyhláška č. 82/2017 Sb., o minimálních technických a organizačních požadavcích na zabezpečení sítí a informačních systémů - tato vyhláška stanovuje konkrétní požadavky na zabezpečení sítí a informačních systémů, včetně požadavků na správu hesel, zálohování, monitorování a dalších aspektů kybernetické bezpečnosti.

Následující instituce mají klíčovou roli v oblasti kybernetické bezpečnosti v České republice:

- Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) - je hlavní institucí odpovědnou za koordinaci a dohled nad kybernetickou bezpečností v České republice. NÚKIB vyvíjí strategie, plány a směrnice pro kybernetickou bezpečnost, provádí analýzy rizik a koordinuje činnost ostatních institucí v této oblasti.
- Národní centrum kybernetické bezpečnosti anýz, sleduje kybernetické hrozby a incidenty, koordinuje reakce na kybernetické incidenty a provádí prevenci a ochranu proti kybernetickým hrozbám.
- Governmental Computer Emergency Response Team (GovCERT) - je český tým specializovaný na kybernetickou bezpečnost, který působí pod NÚKIB. GovCERT monitoruje kybernetické hrozby, reaguje na kybernetické incidenty a poskytuje odbornou pomoc a podporu subjektům kritické infrastruktury při řešení kybernetických událostí.
- Czech Security Incident Response Team (CSIRT.CZ) - je tým specialistů v oblasti kybernetické bezpečnosti, který poskytuje technickou podporu a služby při řešení kybernetických incidentů a zabezpečení sítí a informačních systémů. CSIRT.CZ je součástí NÚKIB a spolupracuje s dalšími národními i mezinárodními týmy pro kybernetickou bezpečnost.
- Národní centrum kybernetické ochrany (NCKO) - je součástí Ministerstva obrany ČR a zajišťuje ochranu a bezpečnost informačních systémů a sítí Ministerstva obrany a dalších vojenských subjektů. NCKO monitoruje kybernetické hrozby, provádí analýzy a reaguje na kybernetické incidenty v oblasti vojenského a obranného sektoru.
- Kybernetická bezpečnostní informační služba (KySIO) - je zvláštní orgán Ministerstva vnitra ČR, který má za úkol provádět kybernetickou obranu a kybernetickou bezpečnost v rámci činností zabezpečování vnitřního pořádku a státní bezpečnosti. KySIO sleduje kybernetické hrozby, provádí analýzy rizik, vyhodnocuje a reaguje na kybernetické incidenty, a koordinuje spolupráci s dalšími subjekty v rámci kybernetické bezpečnosti.
- Minimální bezpečnostní standard je dokument, který stanovuje požadavky na minimální technické a organizační opatření pro zabezpečení sítí a informačních systémů, včetně požadavků na správu hesel,

zálohování, monitorování, šifrování a dalších aspektů kybernetické bezpečnosti. Tento dokument je vydáván NÚKIB a má za cíl podpořit zvýšení úrovně kybernetické bezpečnosti v Č eské republice a zabezpečit ochranu informačních systémů proti kybernetickým hrozbám.

- Doporučení NÚKIB pro administrátory je dokument, který poskytuje konkrétní doporučení a směrnice pro administrátory sítí a informačních systémů, jak správně zabezpečit a chránit své systémy proti kybernetickým hrozbám. Obsahuje praktické rady a postupy pro zajištění bezpečnosti sítí a informačních systémů, včetně oblastí jako jsou správa uživatelských účtů, zálohování, aktualizace softwaru, síťové zabezpečení, monitorování a další.

Příklady českých informačních zdrojů v oblasti kybernetické bezpečnosti mohou zahrnovat:

- Oficiální webové stránky Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) - poskytují informace o aktuálních hrozbách, publikují dokumenty a doporučení týkající se kybernetické bezpečnosti v České republice.
- CSIRT.CZ - oficiální webové stránky českého týmu pro kybernetickou bezpečnost, který poskytuje technickou podporu a služby při řešení kybernetických incidentů. Obsahují informace o aktuálních hrozbách, publikují doporučení a technické rady pro zabezpečení sítí a informačních systémů.
- Kybernetická bezpečnostní informační služba (KySIO) - oficiální webové stránky českého orgánu pro kybernetickou obranu a bezpečnost v rámci Ministerstva vnitra. Poskytují informace o aktuálních hrozbách, publikují zprávy a doporučení týkající se kybernetické bezpečnosti a informačních technologií.
- Národní centrum kybernetické ochrany (NCKO) - oficiální webové stránky českého centra pro ochranu a bezpečnost informačních systémů v rámci Ministerstva obrany. Poskytují informace o kybernetických hrozbách a publikují materiály a doporučení pro zabezpečení vojenských informačních systémů.
- Česká asociace pro kybernetickou bezpečnost (CAKIB) - nezisková organizace, která se zaměřuje na podporu kybernetické bezpečnosti v České republice. Poskytuje informače, zdroje, výcviky a konference týkající se kybernetické bezpečnosti. Jejich webové stránky obsahují informace o nejnovějších trendech, metodách a postupech v oblasti kybernetické bezpečnosti.
- Bezpečnostní expert (www.bezpecnostniexpert.cz) - český informační zdroj zaměřený na bezpečnost IT systémů, s důrazem na kybernetickou bezpečnost. Poskytuje aktualizované informace o hrozbách, bezpečnostních opatřeních, průvodcích a návodech pro zabezpečení informačních systémů.
- Základní a střední školy s informatickým zaměřením - některé české základní a střední školy nabízejí výuku informačních technologií a kybernetické bezpečnosti, které mohou být zdrojem informací a vzdělání v oblasti kybernetické bezpečnosti pro studenty.
- Odborné časopisy a publikace zaměřené na IT a kybernetickou bezpečnost - existuje několik českých odborných časopisů a publikací, které se specializují na témata IT a kybernetické bezpečnosti. Tyto zdroje poskytují aktualizované informace, články a analýzy v oblasti kybernetické bezpečnosti.
- Tyto jsou jen některé příklady českých informačních zdrojů v oblasti kybernetické bezpečnosti. Je důležité sledovat oficiální webové stránky vládních organizací, profesních organizací, vědeckých institucí a dalších relevantních subjektů, které se zabývají kybernetickou bezpečností, aby byla zajištěna aktuálnost a spolehlivost informací.