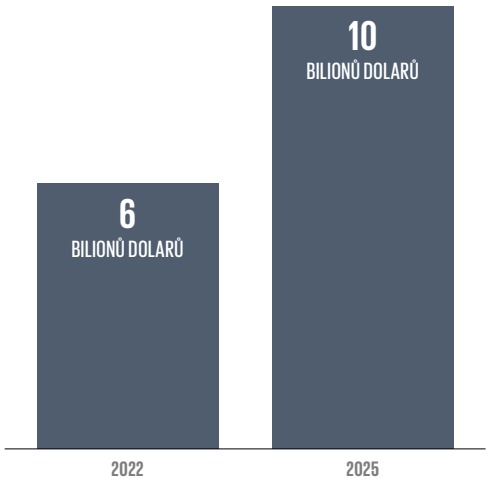
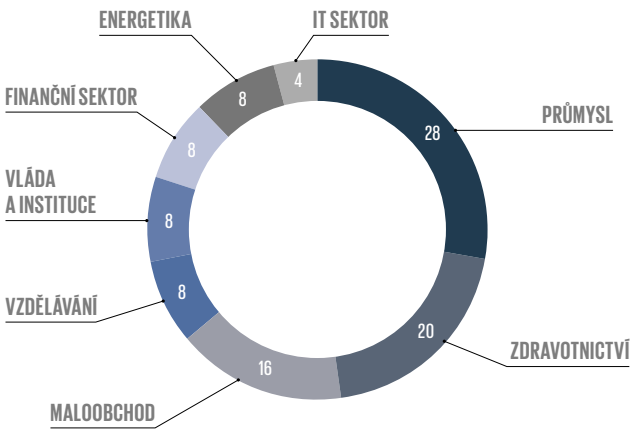
## ZISKY HACKERŮ Z KYBERNETICKÝCH ÚTOKŮ
(celosvětově, za daný rok)




ZDROJ: SOPHOS

## VYDĚRAČSKÉ (RANSOMWARE) ÚTOKY PODLE ODVĚTVÍ (podíl v %)

**Ransomware blokuje počítačový systém nebo šifruje data v něm zapsaná a pak požaduje od oběti výkupné za obnovení přístupu.**




ZDROJ: MICROSOFT

Avšak navzdory odstrašujícím příkladům si české firmy potřebu chránit svá data a systémy často neuvědomují. „Nedávno jsem například mluvil s majitelem jedné dopravní firmy. Má tržby zhruba 4,5 miliardy korun ročně a přes tisíc zaměstnanců. Vůbec nevěděl, jak ve firmě pracují s daty. A když jsem mu řekl, že se může stát, že mu kvůli kybernetickému útoku třeba 14 dní nevyjede žádné auto, divil se proč. Přitom by útočníkům stačilo využít data ze slabě zabezpečeného dispečerského systému a je to," popisuje ředitel Thein Digital Tomáš Budník.

„V tuzemských středních firmách, ale i v řadě větších firem je oblast kybernetické bezpečnosti často řešena jen na bazální úrovni, to znamená firewally, antivirové programy. Nastavení procesů v oblasti detekce, identifikace a řešení incidentů je obvykle nedostatečné. Společnosti nejenže nemají prostředky na technologie, ale především jim chybí odborníci schopní využít výstupy z těchto technologií," uvádí manažer ve společnosti Deloitte Jiří Kaplický.

### ZÁKONEM PŘIMĚT KE ZMĚNĚ

Snaha reagovat na tyto sílící hrozby a zlepšit ochranu proti kybernetickým útokům napříč Evropou se nyní promítá do nové legislativy – evropské směrnice NIS 2 a v Česku pak do nového zákona o kybernetické bezpečnosti, který ze směrnice vychází. Nová regulace má především zvýšit povědomí firem a institucí o kybernetické bezpečnosti a potřebě vyspělé ochrany jejich systémů. Inspirovala se v tom nařízením GDPR, které před pěti lety přimělo pod hrozbou drakonických pokut evropské podniky přejít na nový standard ochrany osobních dat zákazníků a lidí s danou organizací spjatých. Stamilionovými pokutami tak kvůli nedodržení nastoleného standardu ochrany hrozí i nová evropská směrnice v oblasti kybernetické bezpečnosti.

**77**
**procent**
českých firem ročně se stane terčem vyděračského hackerského útoku.

„Je potřeba si uvědomit, že kybernetická bezpečnost je nikdy nekončící proces, kterému je potřeba se věnovat průběžně. S tím je spojena také nezbytná osvěta vedoucích pracovníků i řadových zaměstnanců, aby si uvědomovali rizika spojená s prací v online prostředí," říká o nových pravidlech Marek Vala, mluvčí Národního úřadu pro kybernetickou a informační bezpečnost.

Rozsah konkrétních povinností, které zákon firmám a institucím nově stanoví, bude záležet na tom, do kterého ze dvou režimů budou spadat v případě, že se jich bude týkat zmíněná regulace. Bude existovat užší skupina, na kterou budou kladeny vyšší požadavky – srovnatelné s požadavky stávajícího zákona o kybernetické bezpečnosti, a skupina, na kterou budou kladeny nižší požadavky tak, aby byla finanční a administrativní zátěž pro tyto organizace únosná a přiměřená. Do kterého režimu spadnou, zjistí společnosti z takzvané určovací vyhlášky. Její návrh úřad pro kybernetickou bezpečnost zveřejnil v polovině ledna.

„Nižší režim zákona bude mít volnější požadavky například na hlášení bezpečnostních in-