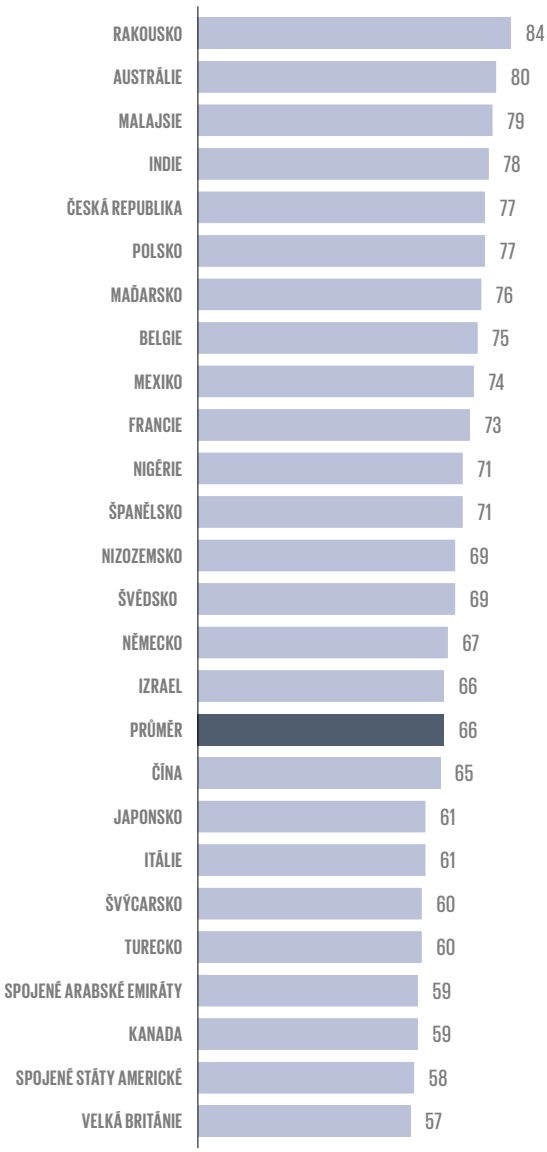
PODÍL ORGANIZACÍ ZASAŽENÝCH VYDĚRAČSKÝM ÚTOKEM
(v procentech, data za rok 2021)



ZDROJ: SOPHOS

cidentů. Subjekty ve vyšším režimu povinností pak musí podle návrhu zákona hlásit veškeré kybernetické bezpečnostní incidenty," uvádí Viktor Paggio, expert poradenské společnosti Deloitte.

Společnosti a instituce spadající do nižšího režimu povinností také budou potřebovat méně specialistů na kyberbezpečnost. Obecně jim stačí expert věnující se kybernetické bezpečnosti. „Ty ve vyšším režimu musí obsadit více rolí manažera kybernetické bezpečnosti, architekta kybernetické bezpečnosti, auditora kybernetické bezpečnosti," dodává Paggio.

295
tisíc dolarů
Taková je průměrná výše výkupného zaplacená českými firmami.

Pro české firmy, a to zejména ty, které dosud pod žádnou regulaci kybernetické bezpečnosti nespadaly, budou nová pravidla znamenat zásadní přerod v přístupu k ochraně IT systémů. Přesný návod na to, co je třeba udělat, ale v zákoně ani ve směrnici nenajdou. Každá společnost by měla být sama schopná identifikovat si kybernetická rizika, která ji trápí. „Směrnice ani návrh tuzemského zákona neříkají, že máte přesně vyjmenovaná primární aktiva nebo podpůrná a ta máte chránit konkrétním způsobem," vysvětluje Ščerba.

Zaměřit se na kybernetickou ochranu přitom organizace nebudou muset jen ve svých vlastních systémech, ale i v celém dodavatelském řetězci. „Zejména se jedná o prověřování bezpečnosti dodavatelského řetězce, skutečné vynucování plnění požadavků na kybernetickou bezpečnost vůči dodavatelům a jejich subdodavatelům a taktéž zjišťování informací o těchto dodavatelích a jejich hlášení Úřadu pro kybernetickou bezpečnost," popisuje partner advokátní kanceláře Sedlakova Legal Bohuslav Lichnovský.

Jenže zástupci firem to často považují za další příklad zbytečné administrativní zátěže, kterou stát dusí byznys. „Je třeba si uvědomit, že malé firmy na toto nemají kapacity, jak personální, tak finanční. Firmy už nebudou mít vůbec čas na svůj hlavní byznys," varuje generální ředitelka Asociace malých a středních podniků Eva Svobodová.

PROSTOR PRO BYZNYS

Nicméně nová pravidla nejde vnímat jen jako „strašáka". Otvírají také prostor pro rozvoj byznysu a nové podnikatelské příležitosti. Podle Ščerby jde o unikátní příležitost prodávat řešení kybernetického compliance, rizikové analýzy či technické dokumentace na klíč.

Například advokátní kancelář Sedlakova Legal plánuje nabídnout aplikaci, která firmám umožní projít jednoduchý check list, na jehož základě zjistí, zda se na ně regulace vztahuje a do jak přísného režimu spadají.

Nová regulace ale také bude s největší pravděpodobností znamenat nebývalou příležitost pro rozvoj cloudových řešení, tedy sdílení pokročilého softwaru vyvinutého velkými hráči na IT trhu.

„Cloud vidíme jako příležitost implementovat chytrá řešení a akcelerovat zavedení bezpečnostních opatření ve společnosti. Nemáme moc času na zavedení nových technologií v menších společnostech. Cloud může pomoci