S novými a rozšířenými standardy kyberbezpečnosti přibude ve firmách administrativy. Budou muset například zpracovávat rizikové analýzy a zajišťovat školení.

dodavatele pitné vody. Ve zdravotnictví už nepůjde jen o poskytovatele zdravotní péče, ale rovněž o laboratoře a firmy výzkumné a vyrábějící v případě ohrožení veřejného zdraví léky a zdravotnické prostředky.

Nově bude vysokou úroveň zabezpečení potřebovat veřejná správa i na komunální úrovni, třeba čističky odpadních vod či poštovní služby. A výrobci počítačů, elektrooptických zařízení a elektroniky, strojů a motorových vozidel či chemičky a potravinářské podniky. Nové povinnosti se dotknou celých dodavatelských řetězců včetně jejich menších subdodavatelů.

Dopad směrnice zaznamená i svět internetu. Dosud se striktní pravidla vztahovala na digitální infrastrukturu, internetové uzly a poskytovatele domén. Pod zákon ale budou zahrnuta datová centra či služby elektronické komunikace. Mírnějšímu režimu začnou podléhat internetové vyhledávače, online tržiště a sociální sítě.

Nedostatek odborníků

S rozšířením povinností – půjde o zpracování analýz rizik, vytipování zranitelných míst, vyhodnocování přijatých opatření, prevenci a odhalování incidentů a jejich hlášení – narostou nároky na administrativu. I podle Svobodové bývají největším nebezpečím nepoučení zaměstnanci a nezbytností bude jejich systematické proškolování. „Zásadní pro mnoho domácích společností bude nedostatek odborníků na informační bezpečnost. Obvyklé obsazení jednoho či dvou specialistů na pokrytí nových požadavků nebude stačit," odhaduje Kudělka z KPMG. Asociace malých a středních podniků se navíc obává, že zbývající IT odborníky „odsají" zahraniční počítačové firmy, které si v Česku otevírají výzkumná a rozvojová centra.

Mnoho společností bude mít nedostatek odborníků na informační bezpečnost. Obvyklé obsazení jednoho či dvou specialistů už nebude stačit.

Menší a méně solventní podniky by proto podle Svobodové neměly podceňovat alespoň základní organizační záležitosti. Tedy to, kdo, kdy a k čemu má přístup a kde například jsou zálohována hesla. „Nezřídka se stává, že firma je po kyberútoku paralyzovaná, protože se vůbec neví, kde a jaká data konkrétně byla," říká.

Hackerských útoků v Česku přibývá. Třeba České dráhy nedávno ohlásily výpadky aplikace Můj vlak a spadly také weby letišť v Karlových Varech, Ostravě a Pardubicích. Útoky na své systémy zaznamenaly i ministerstvo vnitra a Národní úřad pro kybernetickou a informační bezpečnost.