

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **93** ze dne **10.12.2024**

Čtyři přístupy pro zmírnění kybernetických rizik ohrožujících podnikání

Kybernetická rizika jsou zároveň podnikatelská rizika. Cokoliv, co ohrožuje informační technologie, ohrožuje firmu. Podniky se staly extrémně závislé na svých digitálních aktivech a v důsledku toho si jejich vedoucí pracovníci musí uvědomit nutnost rozsáhlých změn.

"Zřejmě nejzásadnější úlohou manažerů pro informační bezpečnost (CISO) je řadit kybernetická rizika podle skutečného dopadu. To vyžaduje stejnou míru porozumění byznysu a technologií, ale i smysl pro to, jak se při útoku chovají objekty, které nikdy nebyly navrženy jako bezpečné. Není to snadný úkol, a to nejen z technologických důvodů. Součástí tohoto hodnocení je nutnost pochopení priorit uvnitř hodnotového řetězce organizace a jejich odpovídajícího zabezpečení," vysvětlil Ondřej Štáhlavský, regionální ředitel společnosti Fortinet pro střední a východní Evropu.

V minulosti byla odolnost spíše technickým konceptem – šlo o navrácení serverů zpět do provozu. Dnes je to zákonný požadavek doložený auditovatelným plánem. Od řady technických kroků jsme se posunuli ke smluvnímu obnovení kritických služeb.

Tyto plány jsou podloženy čtyřmi typy přístupů:

1. **Prioritní obnova** - Velmi citlivý žebříček, který lze vytvořit pouze prostřednictvím pravidelné spolupráce mezi vedením organizace a provozním týmem. Zásadní je zde závěrečné schválení vedením. Jakkoli je obtížné pořadí kybernetických rizik stanovit, jedná se o skutečně jedinečný způsob, který přivádí manažery pro informační bezpečnost a tým do centra dění.
2. **Obranné strategie** - Zhodnocení správné kombinace produktů, služeb, personálního zajištění a procesů je klíčové. Méně je v tomto případě více. Po letech akumulace si kybernetičtí specialisté uvědomili, že velká změň produktů a dodavatelů není příliš efektivní. Příští éra bezpečnosti se bude odehrávat prostřednictvím konvergence, nikoli dalším přidáváním.
3. **Možnosti nabídky** - V tomto případě se jedná o poskytování informací, řady řešení a rozhodnutí, které musí učinit vedení organizace. Součástí práce manažera pro informační bezpečnost je nabízet scénáře jako řadu zdokumentovaných kroků: investice, harmonogram, přínosy a rizika. Pak CISO manažer může navrhnout posloupnost jednotlivých kroků. Výběr dalšího postupu je ale úkolem vedení organizace. Tímto způsobem se CISO manažer stává oprávněnou realizační pákou pro konsensuální rozhodnutí, místo toho, aby byl označen jediným viníkem výsledků.
4. **Výkonné vedení** - Manažer pro informační bezpečnost se musí zodpovídat přímo generálnímu řediteli. Důsledky nejasné nebo rozptýlené podpory přesahují ono nepohodlí pozice; v sázce je totiž přežití celé společnosti. V roce 2024 a v budoucích letech je podřízení kybernetické bezpečnosti jakémukoli jinému hledisku než strategii společnosti zásadní chybou v řízení. Podobnou té, kterou stavitelé lodi Titanic udělali, když vyměnili záchranné čluny za pokoje na sluneční palubě.

"Kybernetická bezpečnost není pouze o vyhýbání se ledovcům. Jedná se o holistický přístup, který zahrnuje všechny aktivní a pasivní dimenze bezpečnosti do jedné integrované platformy. Holistický zde však neznamená monopolní. Fungující starší, zastaralý, nejlepší nebo samostatná řešení jsou životní fakta. Množství technologií, dodavatelů, procesů a rozsah digitálních transformací však volají po zjednodušení. Příliš často se tento chaos

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **93** ze dne **10.12.2024**

mění ve velké incidenty, které fungují jako budíček. Pak nejde o milion, který jsme neutratili, ale o 100 milionů, o které jsme právě přišli," uzavřel Štěhlavský.

Zdroj: AVcentrum ČR