

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **96** ze dne **14.1.2025**

Jak odolat kybernetickým útokům v roce 2025?

Hlavní očekávanou událostí roku 2025 je v oblasti firemního IT souběh dvou dlouho očekávaných zákonů. Prvním je implementace evropské směrnice NIS2, druhým pak novela Zákona o ochraně utajovaných informací. Českým firmám přinesou řadu změn a nových povinností týkajících se kybernetické bezpečnosti, které se dotknou nejen jejich vnitřních procesů, ale také spolupráce s partnery, dodavateli a zákazníky.

"Start dvou tak-to významných zákonů v jednom roce představuje pro firmy ekonomickou, organizační a technologickou zátěž, jaká tu dlouho nebyla," říká Tomáš Hlavsa, bezpečnostní ředitel společnosti Eviden. "Výzvou to bude především pro společnosti, jejichž partnerem je stát. Řadu z nich postaví před dilema, jestli do spolupráce s veřejnou sférou více zainvestovat, nebo se soustředit na byznys v komerční sféře."

Umělá inteligence v první linii

Dalším klíčovým trendem pro následující rok bude umělá inteligence v roli ochránce firemního IT. "Pro řadu odvětví je AI stále ještě mód-ním termínem, který hledá uplatnění. V prostředí kyberbezpečnosti se z umělé inteligence stal standard," upozorňuje Hlavsa. Nasazení AI a strojového učení na počítačovou bezpečnost má hned několik výhod. V oblasti detekce potenciálních hrozeb zvládnou stroje pracovat rychleji, přesněji a levněji než lidé. Dokáží zpracovat kvalitní podklady, které pak může snáze vyhodnotit skutečný člověk. Skvěle fungují jako prvek prediktivní obrany, kdy odhalují útoky ještě před tím, než se stanou. "O skutečném přínosu této technologie vypovídá, že požadavky na AI se už objevují v prvních výběrových řízeních na kybernetické zabezpečení," dodává Hlavsa.

Dlouhá fronta na hackery

Jako třetí velké téma pro rok 2025 vidí Tomáš Hlavsa penetrační testování. Poptávka po práci kvalifikovaných etických hackerů se zvyšuje zejména s přicházející normou NIS2. Penetrační testování je totiž nezbytnou součástí hodnocení odolnosti organizace vůči kybernetickým hrozbám. "V roce 2024 jsme zaznamenali meziroční nárůst poptávky po penetračním testování o 80 %," říká Hlavsa. Za nárůstem vidí zejména fakt, že skutečných odborníků je v Česku málo. Řádově jsou jich jen desítky.

Podle názoru Tomáše Hlavy se bude v roce 2025 zájem klientů dále zvyšovat. "Očekáváme příliv dvou skupin klientů. Jednak to budou ti, kteří etický hacking ještě nepodstoupili. Druhou skupinu budou tvořit ti, kteří již penetrační testování podstoupili, nejsou s jeho výsledkem spokojeni a hledají skutečně kvalitní a důkladnou analýzu. Ta odhalí nejen zranitelnost infrastruktury, ale také ukáže, kudy již unikají data klienta na dark web," uzavírá Tomáš Hlavsa.

Zdroj: AVcentrum ČR