Kdo chce přežít rok 2025, musí do svého IT pustit státní úředníky, umělou inteligenci a hackery, říká expert na kyberbezpečnost

18.12.2024 - | PROTEXT

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 takto 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 podle expertů Eviden umělá inteligence v roli ochránce firemního IT. *„Pro řadu odvětví je AI stále ještě módním termínem, který hledá uplatnění. V prostředí kyberbezpečnosti se z umělé inteligence stal standard,“* upozorňuje Tomáš Hlavsa z Evidenu. 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 Tomáš Hlavsa.

Dlouhá fronta na hackery

Jako třetí velké téma pro rok 2025 vidí experti společnosti Eviden 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 Tomáš Hlavsa. Za nárůstem vidí zejména fakt, že skutečných odborníků je v Česku málo. Řádově jsou jich desítky. Eviden má výhodu v tom, že má vlastní mezinárodní pentestový tým. Jsou v něm experti z Česka, Rumunska, Polska, Německa či Rakouska a budoucí odborníky si vybírá také z řad studentů, které postupně vzdělává.

Podle názoru Tomáše Hlavsy 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 spokojení a hledají skutečně kvalitní a důkladnou analýzu. Ta odhalí nejen zranitelnost infrastruktury, ale také ukáže, kudy již unikají data klienta na dark web,“* uzavírá ředitel kybernetické bezpečnosti společnosti Eviden.

O společnosti Eviden

Společnost Eviden pokrývá oblasti digitálních služeb, velkých dat a bezpečnosti. Eviden je globálním lídrem v oblasti spolehlivé a udržitelné digitální transformace založené na datech. Jako digitální podnik nové generace s celosvětově vůdčími pozicemi v oblasti digitálních technologií, cloudu, dat, pokročilé výpočetní techniky a kybernetické bezpečnosti přináší odborné znalosti pro všechna odvětví ve více než 53 zemích. Spojením špičkových technologií napříč celým digitálním kontinuem a 57.000 specialistů světové úrovně rozšiřuje Eviden možnosti technologií pro podniky a orgány veřejné správy a pomáhá jim budovat jejich digitální budoucnost. Eviden je součástí skupiny Atos s ročním obratem cca 5 miliard eur.

https://www.ceskenoviny.cz/tiskove/zpravy/kdo-chce-prezit-rok-2025-musi-do-sveho-it-pustit-statni-urednik y-umelou-inteligenci-a-hackery-rika-expert-na-kyberbezpecnost/2610650