Studiu EY: Scade încrederea liderilor din domeniul securității cibernetice în sistemele de apărare ale organizației, iar costurile cresc

- **Doar 1 din 5 respondenți consideră că abordarea securității cibernetice în organizația lor în este eficientă**
- **Cheltuielile anuale pentru cibernetică ajung la 35 de milioane de USD, iar costul mediu pentru o breșă de securitate poate să ajungă la 4 milioane de USD**
- **76% dintre respondenți au nevoie de șase luni sau mai mult pentru a detecta și a răspunde la un incident**

Numărul de amenințări cibernetice și costurile asociate sunt în creștere, iar liderii în domeniul securității cibernetice par să se confrunte cu un deficit de eficiență a mijloacelor de apărare din organizațiile lor, potrivit studiului EY 2023 Global Cybersecurity Leadership Insights Study.

Sondajul realizat în rândul a 500 de lideri în domeniul securității cibernetice din întreaga lume arată că doar unul din cinci consideră că abordarea organizației lor este eficientă pentru amenințările actuale și viitoare. Un procent de 50% dintre respondenți par sceptici în ceea ce privește eficiența formării pe care o oferă organizațiile lor și doar 36% sunt mulțumiți de nivelurile de adoptare a celor mai bune practici de către echipele din afara departamentului IT.

În același timp, liderii respondenți raportează costuri tot

mai mari asociate investițiilor în securitate cibernetică și o rată medie de 44 de incidente cibernetice în 2022. Respondenții Chief Information Security Officer (CISO) raportează cheltuieli medii anuale de 35 milioane USD pentru securitatea cibernetică, iar costul mediu al unei breșe pentru organizația lor a crescut cu 12%, ajungând la 2,5 milioane USD în 2023 și se anticipează că va ajunge la 4 milioane USD.

În ciuda nivelurilor ridicate de cheltuieli, timpii de detectare și de răspuns par să fie lenți. Mai mult de trei sferturi dintre respondenți (76%) spun că organizațiile lor au nevoie în medie de șase luni sau mai mult pentru a detecta și a răspunde unui incident.

Cătălina Dodu, liderul departamentului de Consultanță, EY România și Cybersecurity Leader EY South Cluster: *„Cu o astfel de creștere a tipului, complexității și numărului de atacuri, observăm că responsabilii CISO se simt încă nepregătiți în faţa acestor amenințări cibernetice. Nu este vorba doar despre cât de mare este investiția în protejarea organizațiilor, ci mai mult despre cât de bine este extrasă valoarea din soluții inteligente specifice. O securitate cibernetică eficientă este ceea ce ar trebui să fie scopul nostru – o mai bună integrare și utilizare a tehnologiilor de securitate cibernetică, împreună cu o cultură de excepție în ceea ce privește elementele de bază ale securității cibernetice este ceea ce poate face diferența în protejarea organizațiilor*”.

Simplificare pentru supraviețuire

Studiul constată că acele organizații care sunt mai mulțumite de abordarea lor în securitate cibernetică, care se confruntă cu mai puține incidente cibernetice și care pot detecta și răspunde mai repede la incidente au anumite caracteristici comune.

Cei 70% dintre acești „creatori de siguranță” identificați în studiu, se definesc ca fiind primii care adoptă tehnologii

emergente, se concentrează pe extragerea celei mai mari valori din soluții avansate specifice, cum ar fi inteligența artificială/învățarea automată (AI/ML) (62%) și Securitate, Orchestrare, Automatizare și Răspuns (SOAR) (52%), care le permit să aibă o vedere clară asupra incidentelor de securitate cibernetică. În plus, aceștia dispun de strategii specifice pentru gestionarea atacurilor prin intermediul mai multor surse: propriul cloud, partenerii lor și prin intermediul lanțurilor lor de aprovizionare. Respondenții din aceste tipuri de organizații par aproape de două ori mai susceptibili de a fi foarte preocupați de riscurile cibernetice din lanțul lor de aprovizionare (38%) și de riscurile conexe, cum ar fi protecția proprietății intelectuale (38%).

Acești „creatori de siguranță” integrează gândirea și formarea în domeniul securității cibernetice de la nivelul conducerii până la fiecare angajat al organizației. Ca urmare, respondenţii CISO din aceste companii spun că este mai probabil ca abordarea lor să aibă un impact pozitiv asupra ritmului lor de transformare și inovare (56%), precum și asupra capacității lor de a răspunde rapid la oportunitățile pieței (58%) și de a se concentra pe crearea de valoare (63%).