Cost of a Data Breach Report 2026 | IBM

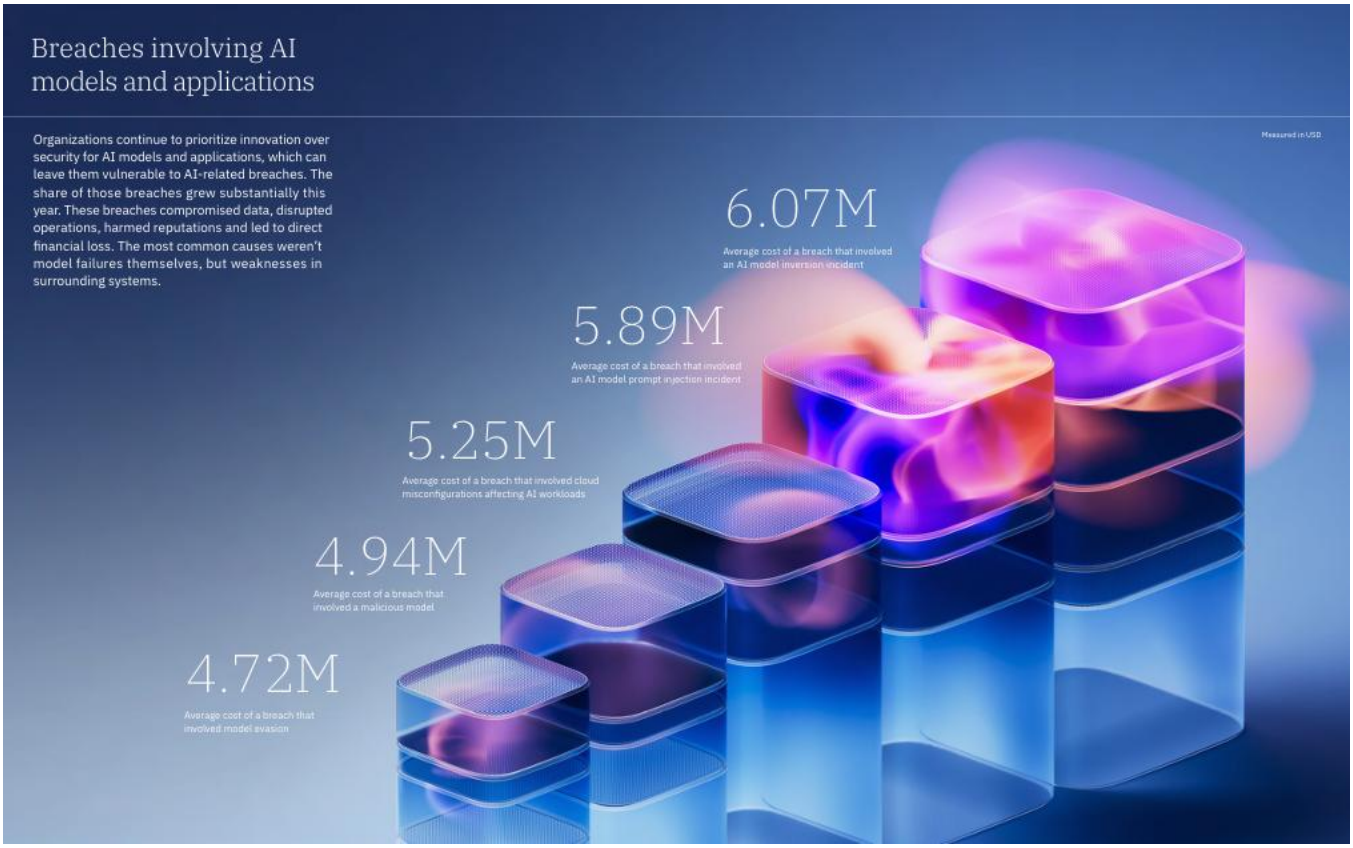
- **Punctul de cotitură al Inteligenței Artificiale**

Raportul integral si webinar explicativ aici: https://www.ibm.com/reports/data-breach

Cea de-a 21-a ediție anuală a raportului *Cost of a Data Breach* (2026) relevă o intensificare a curbei atacurilor bazate pe inteligența artificială – fenomenul căpătând un caracter exponențial prin tool-uri ca Mythos, cu o creștere de 68% de la an la an a atacurilor generate de AI, fapt ce evidențiază amploarea tot mai mare a amenințărilor. Raportul din acest an subliniază impactul financiar și operațional al acestor atacuri, punând accent pe necesitatea ca organizațiile să își alinieze investițiile în securitate la ritmul accelerat al amenințărilor generate de inteligența artificială.

4,99 mil.$	6 mil.$	65zile	41%
Costul mediu global al unei breșe de securitate a datelor, in crestere cu 12% fata de anul precedent	Costul mediu al atacurilor bazate pe tehnica de inversare a modelelor AI	Reducerea duratei de gestionare a breselor prin utilizarea la scara larga a AI automatizat (reducere cost cu 1,93 m$)	Ponderea atacurilor de tip ransomware care au inclus daune la adresa reputației brandului

50%	56%	92%	85%
Ponderea organizațiilor care implementează agenți AI în centrele lor de operațiuni de securitate (SOC)	Creștere a atacurilor generate cu AI, adăugand o medie de 1 mil. $ cost adițional per incident de securitate.	Ponderea organizațiilor care au raportat o breșă de securitate legată de AI și nu dispuneau de controale adecvate privind accesul la AI	Ponderea organizațiilor care intenționează să majoreze cheltuielile pentru securitate ca răspuns la amenințările asociate modelelor AI de ultimă generație



Pe măsură ce modelele AI de ultimă generație comprimă intervalul dintre descoperirea unei vulnerabilități și exploatarea acesteia – accelerând atacurile de la viteza umană la cea a puterii de calcul moderne – costul întârzierii se va măsura în minute, nu în luni.

Eșecurile legate de întârzierile în detectare, lacunele în izolare, deplasarea laterală, utilizarea abuzivă a credențialelor și latența în luarea deciziilor au acum un impact mult mai grav și mai costisitor asupra organizațiilor. Studiul din acest an confirmă această concluzie.

RECOMANDARI: Pentru a ajuta la prevenirea și atenuarea incidentelor de securitate, la reducerea costurilor asociate acestora – precum și pentru a pregăti organizațiile pentru era securității la viteza calculatoarelor – experții IBM propun următoarele patru abordări eficiente:

- ***Gestionarea securității la viteza actuală a atacurilor***

Un punct de plecare adecvat este aplicarea inteligenței artificiale de tip „agentic" în domeniul gestionării vulnerabilităților. Acest segment a devenit o țintă vulnerabilă din cauza capacităților modelelor AI de ultimă generație de a identifica vulnerabilități critice în principalele sisteme de operare și browsere. Prin integrarea AI în întregul ciclu de viață al securității, companiile își pot transforma programele de securitate în sisteme coerente, capabile de o apărare continuă și autonomă. Această abordare presupune utilizarea AI pentru a analiza expunerile, a aplica politici și a coordona procesele de detectare și izolare cu o intervenție umană minimă, reducând astfel intervalele de vulnerabilitate și accelerând izolarea atacurilor care se propagă rapid. Adoptând aceste măsuri de securitate bazate pe AI, companiile își pot consolida reziliența, pot eficientiza conformitatea și se pot asigura că sunt pregătite să contracareze rapid amenințările alimentate de inteligența artificială.

- ***Trecerea securității identității la verificare continuă, în timp real***

Securitatea identității rămâne subfinanțată, în ciuda dovezilor tot mai numeroase ale importanței sale. Printre organizațiile care au suferit breșe legate de inteligența artificială în studiul din acest an, 92% nu dispuneau de controale de acces adecvate. Această constatare dezvăluie un eșec sistemic în tratarea identității ca infrastructură critică pentru misiune. În cursa pentru implementarea agenților de inteligență artificială pentru automatizarea proceselor de afaceri - inclusiv operațiunile de securitate care se apără împotriva modelelor de inteligență artificială de frontieră - echipele trebuie să transforme fundamental sistemele de identitate pentru a securiza nu doar oamenii, ci și instituțiile naționale de sănătate (NSH). Această transformare a identității va necesita:

- Descoperirea și integrarea agenților
- Delegarea și autorizarea autentificării
- Detectarea anomaliilor și remedierea riscurilor
- Guvernanță și controale ale ciclului de viață

Această transformare va înlocui abordările tradiționale cu principii moderne de tip „zero trust".

- ***Consolidarea controlului asupra AI prin suveranitatea AI***

Pe măsură ce organizațiile extind utilizarea AI la nivelul platformelor, al infrastructurilor cloud și al ecosistemelor, acestea pot pierde controlul asupra modului în care funcționează modelele și asupra modului în care datele sunt transformate și accesate. Această provocare sporește riscul de breșe de securitate și complică gestionarea răspunsului la acestea. De aceea, suveranitatea AI – menținerea controlului asupra locului în care rulează sistemele IA, asupra modului în care sunt prelucrate datele și asupra persoanelor care au acces la acestea – a devenit acum un imperativ critic de securitate.

- ***Pregătiți-vă pentru riscurile de securitate din era post-cuantică***

Deficiențele fundamentale în gestionarea criptării și a criptografiei lasă organizațiile vulnerabile, chiar dacă investițiile în securitatea rezistentă la tehnologia cuantică au început să crească. De exemplu, doar 37% dintre organizațiile care s-au confruntat cu o breșă de securitate au raportat că criptau datele sensibile la momentul producerii incidentului. În același timp, doar 34% au declarat că dispuneau de măsuri de control pentru monitorizarea și securizarea activelor criptografice – precum cheile și certificatele – în cadrul infrastructurilor lor.