

Inteligenţa artificială a deschis o nouă eră a războiului cibernetic

O breşă ascunsă în PHP mai bine de un deceniu a devenit, în octombrie, o problemă de securitate la scară globală. Descoperirea arată că inteligenţa artificială poate accelera identificarea punctelor slabe din infrastructura digitală, dar şi că timpul de reacţie al companiilor devine o resursă tot mai greu de câştigat.

În lumea digitală, o vulnerabilitate nu trebuie să fie nouă pentru a deveni periculoasă. Uneori, este suficient ca cineva să descopere, după zece sau cincisprezece ani, cum poate fi exploatată. Iar atunci când instrumentele de inteligenţă artificială intră în ecuaţie, distanţa dintre identificarea unei slăbiciuni şi transformarea ei într-un risc concret pentru companii se poate reduce dramatic.

Un astfel de scenariu a devenit realitate în octombrie, când două vulnerabilităţi din limbajul de programare PHP, existente de mai bine de zece ani, au declanşat o cursă internaţională pentru protejarea sistemelor informatice. Cazul, asociat denumirii PHP2Shell, nu reprezintă doar un episod tehnic destinat specialiştilor în securitate cibernetică. El ridică o problemă de interes pentru întreaga economie digitală: cât de pregătite sunt organizaţiile să reacţioneze atunci când o ameninţare veche este descoperită şi exploatată într-un ritm pe care procedurile lor interne nu îl pot urma?

Potrivit informaţiilor comunicate de compania românească Zitec, datele despre vulnerabilităţile înregistrate cu identificatorii CVE-2026-109618 şi CVE-2026-109619 au fost făcute publice la 20 octombrie, iar echipa PHP a publicat actualizările de urgenţă pe 21 octombrie, cu o zi înainte de termenul planificat.

Fereastra de reacţie a fost, aşadar, extrem de scurtă. Pentru administratorii de sisteme şi echipele de securitate, problema nu s-a rezumat la instalarea unui patch. A fost nevoie de identificarea serverelor afectate, evaluarea riscurilor, aplicarea măsurilor temporare de protecţie şi testarea actualizărilor înainte de implementarea lor în mediile de producţie.

Miza este considerabilă. Conform datelor W3Techs citate de Zitec, PHP este utilizat de 69,3% dintre site-urile pentru care este cunoscut limbajul de programare folosit pe server. O vulnerabilitate într-o asemenea componentă poate avea consecinţe dincolo de o singură aplicaţie sau de o anumită companie.

(continuare în pagin 70)

(urmare din pagina 69)

AI schimbă regulile jocului

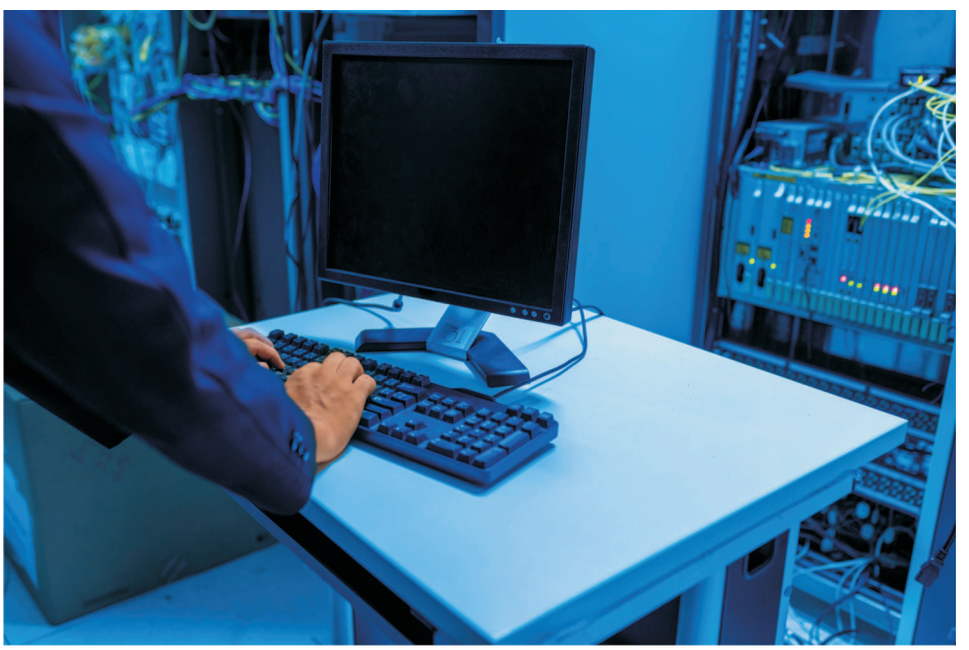
Cea mai importantă particularitate a acestui caz este rolul inteligenţei artificiale în descoperirea vulnerabilităţilor. Potrivit experţilor Calif, companie din California specializată în testarea de securitate a sistemelor AI, comportamentul care stătea la baza problemei fusese semnalat încă din 2020, într-un raport de eroare, fără să conducă la rezolvarea vulnerabilităţii. În 2024, în timpul primului audit extern de securitate al PHP, un dezvoltator din echipa de bază observase, de asemenea, indicii relevante, conform informaţiilor atribuite PHP Foundation. Descoperirea decisivă a venit însă în august 2026, când echipele Wiz, Google, OpenAI şi Calif au identificat vulnerabilităţile cu ajutorul unor instrumente de inteligenţă artificială. Informaţiile au fost păstrate confidenţiale până la pregătirea actualizărilor de securitate.

Semnificaţia acestui episod depăşeşte capacitatea modelelor AI de a analiza cantităţi mari de cod. Astfel de instrumente pot ajuta la identificarea unor relaţii între componente, la recunoaşterea unor tipare periculoase şi la investigarea unor comportamente pe care verificările tradiţionale nu le-au semnalat la timp.Un cod care a trecut ani întregi prin procese de întreţinere şi verificare poate ascunde, în continuare, o slăbiciune exploatabilă. Inteligenţa artificială poate scurta drumul până la descoperirea ei, inclusiv prin reconstruirea modului în care diferite componente interacţionează.

Această capacitate are două feţe. Folosită de echipele de apărare, AI poate accelera auditarea codului, detectarea anomaliilor şi pregătirea măsurilor de remediere. În mâinile atacatorilor, aceleaşi progrese pot facilita identificarea vulnerabilităţilor şi dezvoltarea unor metode de exploatare. Nu înseamnă că orice model de inteligenţă artificială poate compromite automat un server sau că toate vulnerabilităţile pot fi transformate imediat în atacuri funcţionale. Înseamnă însă că avantajul oferit de timpul necesar pentru descoperirea unei breşe nu mai poate fi considerat o protecţie suficientă.

Certificatele digitale, o altă verigă vulnerabilă

Incidentul PHP nu a fost singura problemă de securitate importantă semnalată în aceeaşi perioadă. Între 17 şi 20 octombrie, au apărut informaţii potrivit cărora cheile private asociate unui număr de opt certificate digitale fuseseră compromise. Astfel de chei pot fi folosite pentru emiterea unor certificate false, capabile să facă un site controlat de atacator să pară legitim în anumite condiţii.Certificatele digitale reprezintă una dintre componentele fundamentale ale încrederii în internet. Ele contribuie la autentificarea site-urilor şi la stabilirea conexiunilor securizate dintre utilizatori şi servicii. Compromiterea cheilor private poate pune sub semnul întrebării această încredere, mai ales dacă certificatele afectate sunt acceptate în continuare de aplicaţii sau sisteme. În cazul menţionat, browserele majore au blocat certificatele afectate, eMudhra le-a revocat, iar proiecte precum Composer, managerul de pachete al ecosistemului PHP, şi-au actualizat listele de certificate de încredere. Conform informaţiilor atribuite eMudhra, numai unul dintre cele opt certificate era utilizat într-un mediu de producţie şi niciunul nu emisese certificate către utilizatori finali. Episodul demonstrează că securitatea digitală nu depinde exclusiv de identificarea şi corectarea erorilor din cod. Ea presupune şi protejarea identităţilor digitale, gestionarea certificatelor, actualizarea listelor de încredere şi verificarea permanentă a componentelor de care depind aplicaţiile.



Securitatea cibernetică devine o problemă de conducere

Lecţia principală a incidentului nu este că inteligenţa artificială ar fi făcut internetul, dintr-odată, nesigur. Vulnerabilităţile au existat, iar sistemele digitale au avut întotdeauna puncte slabe. Schimbarea constă în ritmul în care acestea pot fi identificate, analizate şi, eventual, exploatate.

În aceste condiţii, securitatea cibernetică nu mai poate fi tratată exclusiv ca o responsabilitate a departamentului IT. Ea ţine de continuitatea afacerii, de protejarea datelor, de relaţia cu clienţii şi de capacitatea conducerii de a lua decizii rapide atunci când informaţiile sunt incomplete.

Companiile au nevoie de inventare actualizate ale infrastructurii, de proceduri clare pentru instalarea corecţiilor, de monitorizarea vulnerabilităţilor din componentele externe şi de planuri de reacţie testate periodic. În plus, listele de certificate de încredere din aplicaţii, biblioteci şi containere trebuie menţinute la zi, inclusiv atunci când browserele au implementat deja propriile măsuri de protecţie. La fel de importantă este capacitatea de a decide rapid ce trebuie oprit, ce poate continua să funcţioneze şi ce resurse trebuie mobilizate pentru limitarea unui incident. Aceste decizii nu pot fi improvizate în mijlocul unei crize.

Inteligenţa artificială poate deveni un aliat important în identificarea vulnerabilităţilor şi în automatizarea răspunsului defensiv. Dar beneficiile sale depind de infrastructura organizaţiei, de calitatea procedurilor şi de capacitatea oamenilor de a interpreta corect rezultatele furnizate de instrumentele automate.