

**Noua prioritate în apărarea cibernetică: accentul se mută de la rețea, la utilizatori și la accesul lor la resursele companiei**

*Material de opinie de Mihai Olteanu, Director Cyber Defense Advisory, Deloitte România*

Contextul actual, caracterizat prin combinația dintre munca la birou și munca la distanță, nevoia angajaților de a accesa din orice loc echipamentele, rețelele și aplicațiile companiei, folosirea echipamentelor personale pentru îndeplinirea sarcinilor de serviciu (*bring your own device - BYOD*) și utilizarea de soluții *cloud*, a obligat companiile să-și regândească abordarea în domeniul apărării cibernetice. Accentul se mută acum de la parametrii legați de rețea, la modul în angajații pot accesa și utiliza resursele companiei. Arhitectura de tip *Zero Trust,* un concept care implică o abordare integrată a politicilor de guvernanță și a administrării identității în cadrul unei companii, este un exemplu de soluție pentru noile provocări cu care se confruntă companiile.

Construirea unei arhitecturi *Zero Trust* este posibilă cu ajutorul unor [soluții pentru managementul identității (*identity Access Management* – *IAM*) și al accesului privilegiat (*Privileged Access Management – PAM)*](https://www2.deloitte.com/ro/en/pages/technology/solutions/identity-privileged-access-management.html?nc=42)*,* care definesc nivelul și perioada de acces al unui utilizator la resursele organizației. În prezent, necesitatea adoptării unor astfel de soluții a crescut considerabil, având în vedere gradul de încărcare a departamentelor de IT și securitate din organizații, responsabile cu acordarea acestor privilegii în mod manual sau automat, aspect care îngreunează alocarea rapidă a accesului pentru anumiți utilizatori.

Cum poate fi implementată o soluție de gestionare a identității și a privilegiilor acordate utilizatorilor? Companiile trebuie să aibă în vedere trei dimensiuni pentru a crea o arhitectură de tip *Zero Trust.*

**Acces doar la resursele absolut necesare**

În primul rând, să își propună să aibă **în cadrul organizației utilizatori cu acces la un nivel minim necesar (*least privileges)****.* Spre exemplu, noii angajați ar trebui să primească permisiunea de a accesa un număr cât mai redus de resurse; în numeroase companii, abordarea este la polul opus - aceștia primesc acces încă din prima zi la cât de multe resurse posibil, pentru a evita încărcarea ulterioară a departamentului IT sau de securitate. Aceste departamente ar trebui să aibă **o imagine de ansamblu a drepturilor de acces pentru fiecare utilizator** prin construirea unui inventar cât mai clar al resurselor din companie, de la aplicații, la date, la centralizarea și gruparea tuturor drepturilor de acces ce pot fi alocate utilizatorilor într-un catalog de servicii, cu scopul de a îmbunătăți procesul de acordare a permisiunilor. În acest sens, este importantă implementarea unui portal de tip *self service*, cu ajutorul căruia orice utilizator poate cere permisiunile respective, utilizând unul din cele două tipuri de fluxuri – cu auto-aprobare sau cu aprobare prin intermediul unui factor uman decizional.

**Cum arată „viața” unui utilizator**

În al doilea rând, companiile trebuie să acorde o atenție sporită **manierei în care definesc ciclul de viață pentru fiecare utilizator**, de la stabilirea proprietarului unei resurse, până la determinarea unui proces de aprobare pentru a avea control asupra oricăror schimbări survenite în atribuțiile angajatului, și crearea unui catalog complex și granular de permisiuni care pot fi cerute de orice utilizator. Este important ca organizațiile să ia în calcul implementarea unor controale predictive pe întreg procesul de acordare a accesului utilizatorilor, capabile să optimizeze timpul de intervenție umană, și a unor reguli pentru a preveni situații periculoase, precum cea în care un utilizator ajunge să dețină puteri absolute pe linia sa de business (de exemplu, apariția unei persoane care poate iniția plăți pe care apoi le poate și aproba).

**Optimizare, optimizare, optimizare**

De asemenea, organizațiile trebuie să **optimizeze modul în care stabilesc nivelul de acces al fiecărui utilizator** **și timpul petrecut de aprobatori în procesul de acordare a accesului**. O soluție de gestionare a identității și a privilegiilor acordate utilizatorilor poate ajuta în acest sens prin recomandarea unui anumit set de permisiuni în baza unui tipar identificat cu ajutorul inteligenței artificiale. Spre exemplu, dacă 95% din personalul departamentului de contabilitate are aceleași permisiuni, automat, când în organizație va ajunge un nou membru al acelui departament, acesta va avea acces la aceleași resurse ca restul echipei, conform recomandării soluției de inteligență artificială.

În concluzie, implementarea unor soluții de management al identității și al accesului privilegiat a devenit o nevoie stringentă în contextul actual pentru a putea păstra un nivel optim de securitate în cadrul organizațiilor. În contextul creșterii masive a complexității infrastructurilor digitale din organizații, lipsa unor astfel de soluții va duce la atragerea unor atacatori externi sau interni care pot profita de lipsa unor controale riguroase.