

Costul incidentelor cu angajatii care pleaca din companie s-a majorat cu 31%, în trei ani (analiza)

Costul incidentelor legate de personalul intern a crescut cu 31% în perioada 2018 - 2020, pâna la aproape 11,5 milioane de dolari, arata datele centralizate de Eset, compania specializata în securitate cibernetica.

Conform unei analize publicate, recent, pe blogul Eset din România, multe organizatii (43%) nici macar nu au o politica care sa le interzica membrilor din personal sa plece cu datele de lucru ale companiei. Totodata, în Marea Britanie, doar 47% dintre companii interzic accesul ulterior în sediile centrale sau teritoriale ca parte a procesului de offboarding, în timp ce 62% revendica dispozitivele corporative.

"Pandemia COVID-19 a creat conditiile perfecte pentru aparitia de noi riscuri de securitate din interior. Crizele financiare au dus în trecut la o crestere a numarului de fraude si a activitatilor nefaste, asadar este rezonabil sa presupunem ca valul de locuri de munca pierdute si incertitudinea aparuta la începutul anului 2020 au condus în aceeasi directie. În acelasi timp, companiile nu au fost niciodata mai expuse, prin lanturi extinse de aprovizionare si parteneriate, precum si prin infrastructura lor de lucru de la distanta si cloud - o mare parte dintre acestea fiind construite rapid ca raspuns la pandemie. Concluzia este ca, prin decizii premeditate sau accidental, angajatii care demisioneaza pot ajunge sa provoace daune financiare si reputationale semnificative daca riscurile nu sunt atenuate corespunzator. Costul incidentelor legate de personalul intern a crescut cu 31% între 2018 si 2020, ajungând la aproape 11,5 milioane de dolari. Acest lucru face ca procesele eficiente de offboarding sa fie o parte esentiala a oricarei strategii de securitate - dar care este totusi prea des trecuta cu vederea", scriu expertii Eset.

În acelasi context, aproape jumatate dintre angajatii care pleaca (45%) descarca, salveaza, trimite sau extrage documente legate de locul de munca înainte de a parasii compania, iar acest lucru se întâmpla cel mai frecvent în sectoarele de tehnologie, servicii financiare si de afaceri, consultanta si management.

"Fie ca iau aceste informatii cu ei pentru a impresiona un nou angajator, fie ca le fura sau le sterg ca urmare a unei actiuni de razbunare, impactul potential asupra organizatiei este sever. O încălcare grava a confidentialitatii datelor ar putea duce la: cheltuieli de investigare, remediere si curatare a efectelor, cheltuieli judiciare care decurg din actiunile colective, amenzi de reglementare de tipul GDPR si nu numai, daune de brand si reputatie, respectiv avantaje competitiv pierdute", semnaleaza analiza.

În ceea ce priveste drepturile salariatilor referitoare la aportul lor în companie, aproximativ trei sferturi (72%) dintre acestia sunt de parere ca datele pe care le creeaza la locul de munca le apartin (liste de clienti, proiecte de inginerie etc.).

"Pe masura ce organizatiile se pregatesc pentru a face fata lumii post-pandemice, competitia pentru atragerea de noi clienti va fi mai acerba ca niciodata. Tocmai de aceea companiile nu își pot permite sa se confrunte cu astfel de probleme de securitate a datelor care pot proveni dinspre angajatii care pleaca. Ele pot conduce usor la daune financiare si reputationale care ar putea rezulta din încălcarea grava a confidentialitatii datelor. Procesul de offboarding, desi este o mica piesa a puzzle-ului de securitate, este una extrem de importanta", sustin specialistii.

Eset a fost fondata în anul 1992 în Bratislava (Slovenia) si se situeaza în topul companiilor care ofera servicii de detectie si analiza a continutul malware, fiind prezenta în peste 180 de tari. A