Bitdefender

Adăugarea unor paravane avansate de protecție pentru consolidarea ultimului front: criptarea și administrarea patch-urilor

Într-un mediu din ce în ce mai ostil, în care atacurile cibernetice de proporţii ajung la ştiri aproape în fiecare săptămână, companiile au început să-și orienteze paradigma de securitate către obţinerea unei vizibilităţi mai mari asupra modului de desfășurare a atacurilor și modului în care pot deveni victime ale acestora. Recunoscând că producerea unei breșe de securitate a datelor este inevitabilă și adoptând instrumente utile de detecţie și răspuns la nivelul staţiilor de lucru, CISO se concentrează pe minimizarea suprafeţei de atac, adăugând protecţie suplimentară pentru infrastructura lor. Iată unde administrarea patch-urilor și criptarea fac diferenţa.

ASCUNDEREA DATELOR VALOROASE

Un sondaj Bitdefender efectuat asupra unui număr de 1051 de profesioniști în materie de securitate IT din SUA și Europa a evidenţiat că patru din cinci CISO consideră că criptarea reprezintă cel mai eficient mecanism de securizare a datelor, urmat de programele software de securitate și backup-uri. În ceea ce privește datele la nivel de ţară, cel mai ridicat nivel de încredere în criptare se înregistrează în Italia, Regatul Unit și SUA, însă, în medie, numai o singură companie din șase își criptează toate datele.
Trei din patru factori de decizie în materie de securitate IT menţionează costurile financiare și deteriorarea reputaţiei afacerii ca fiind cele mai devastatoare consecinţe cu care s-ar confrunta în cazul în care o ameninţare avansată dobândește acces la „bijuteriile Coroanei”.
Datele de importanţă critică legate de proprietatea intelectuală trebuie stocate local, iar accesul la acestea trebuie restricţionat și permis numai personalului autorizat. Orice date stocate local sau în cloud trebuie să fie criptate pentru a se asigura că infractorii cibernetici nu le pot citi în cazul unor breșe de securitate a datelor sau în caz de acces neautorizat.

CISO trebuie să evite riscul pierderii datelor și să respecte reglementările prin criptarea completă a unităţii de disc a dispozitivelor mobile.

GravityZone Full Disk Encryption protejează datele la nivelul întregii unităţi de disc a staţiei de lucru prin valorificarea mecanismelor de criptare furnizate de Windows (BitLocker) și Mac (FileVault). Acesta profită de criptarea nativă a dispozitivelor pentru a asigura compatibilitate maximă și performanţe sporite. Modulul GZ Full Disk Encryption este integrat în consola și agentul GravityZone, fără a fi necesară configurarea unui agent suplimentar sau instalarea unui server de administrare de chei. Utilizarea infrastructurii existente de securitate a staţiilor de lucru pentru administrarea modulului Full Disk Encryption permite configurarea complet centralizată, cu efort administrativ minim.

FIX CE LIPSEA

Întrucât sistemele fără patch-uri expun organizaţiile la riscuri precum incidente sau epidemii de malware și breșe de securitate a datelor, jumătate din numărul CISO care au participat la sondaj recunosc că extinderea infrastructurii a extins suprafaţa de atac a companiei. Specialiștii în securitate recomandă ferm CISO să actualizeze în permanenţă toate programele software cu cele mai recente patch-uri. Instrumentele de administrare a patch-urilor facilitează această operaţiune și ajută companiile să evite evenimente negative, precum bine-cunoscutele atacuri WannaCry și GoldenEye.

Modulul GravityZone Patch Management permite atât aplicarea automată a patch-urilor, cât și cea manuală. Acesta oferă organizaţiilor un plus de flexibilitate și eficienţă în administrarea patch-urilor, asigurând posibilitatea de a crea un inventar de patch-uri, de a programa scanarea patch-urilor, de a limita aplicarea automată a patch-urilor în cazul aplicaţiilor preferate de administratori, de a diversifica programarea patch-urilor de securitate și non-securitate și de a amâna repornirea sistemului în cazul patch-urilor care necesită o repornire.

În peisajul actual al securităţii cibernetice, aplicarea patch-urilor pentru sistemele de operare și aplicaţii a devenit o prioritate importantă pentru echipa IP atât din motive de securitate, cât și din motive de conformitate. Modulul GravityZone Patch Management permite verificarea aplicării patch-urilor la nivelul întregii companii în vederea respectării politicilor și reglementărilor.