TIP SHEET

5 moduri în care atacurile ransomware afectează backup-ul... Și cum poți preveni aceasta

Soluțiile de backup și recuperare sunt concepute pentru a-ți proteja organizația, dar programele malware sofisticate precum Locky și Crypto vizează acum datele tale de backup. Deloc surprinzător, având în vedere creșterea frecvenței și a amplorii atacurilor ransomware. Prima plată după un atac ransomware – anul 1989 – a pregătit terenul pentru ca hackerii de pretutindeni să înceapă să blocheze datele țintelor nepregătite și să le păstreze până când proprietarii plătesc pentru a și le recupera. Acum, analiștii prezic că un atac ransomware asupra companiilor va avea loc la fiecare 14 secunde - cu un cost de miliarde pentru organizațiile globale. De aceea, este important să ții cont de aceste cinci aspecte atunci când planifici cum să previi, să detectezi și să răspunzi rapid la un atac ransomware asupra backup-ului tău:

1. Atacurile ransomware sofisticate transformă polița ta de asigurare – backup-urile – într-o verigă slabă

Infractorii cibernetici vizează acum în mod agresiv datele de backup ale copiilor shadow – pentru a obține controlul complet sau, mai rău, pentru a distruge ceea ce a fost considerat mult timp drept asigurarea ta pentru continuitatea activității. Atacurile lor tot mai sofisticate intră într-un mediu primar dintr-un punct final și se îndreaptă direct către backup-urile tale – acolo unde sunt stocate acum 80% din datele firmei – ștergând sau compromițând totul de acolo, înainte de a prelua mediul de producție. Ce este necesar pentru a preveni ca atacul ransomware să îți afecteze backup-ul este o apărare pe mai multe niveluri. Joburile originale de backup trebuie să fie păstrate într-o stare protejată și să nu fie niciodată accesibile, pentru a nu fi apelate de un sistem extern. De asemenea, autentificarea cu mai mulți factori (MFA) și capabilitățile de tip scriere-odată-citire-multiplă (WORM) pentru un snapshot sunt caracteristici obligatorii.

Ransomware în cifre

- Un atac ransomware la fiecare 14 secunde
- 700% creștere din 2016
- 35% dintre atacatori primesc banii
- 2 mld USD pierderi financiare
- 11 mld USD pierderi financiare, de productivitate și opriri!

"Programatorii de ransomware știu că backup-urile sunt o protecție reală și de aceea își modifică malware-ul pentru a identifica și elimina backup-urile."

—CSO MAGAZINE

Contactează echipa noastră pentru a afla mai multe

info@m247.ro +4 031 630 2051 m247.ro

5 moduri în care atacurile ransomware afectează backup-ul... și cum poți preveni aceasta

2. Amploarea tot mai mare a atacurilor expune backup-urile la atacuri ransomware

Creșterea explozivă a datelor (IDC estimează că vor exista peste 175 de zetabiți de date până în 2025) și fragmentarea masivă a datelor – proliferarea crescândă a datelor de backup în diferite centre întinse – contribuie împreună la creșterea suprafeței de atac a firmei tale. Drept urmare, datele tale de backup au devenit mai accesibile infractorilor cibernetici. Împiedicarea succesului unui atac ransomware începe în primul rând cu reducerea suprafeței de atac din firmă și cunoașterea datelor pe care le ai și a locului unde se află. O soluție unificată pentru conectarea infrastructurii, a volumelor de lucru și a locațiilor de backup protejează organizația împotriva atacurilor ransomware, prin eliminarea fragmentării masive a datelor.

3. Atacurile asupra backup-urilor sunt facilitate de monitorizarea intermitentă

Amenințările cibernetice nu provin întotdeauna din afara unei organizații; ele pot fi lansate și din intern. Imaginează-ți un angajat nemulțumit care încearcă să modifice sau să șteargă un set mare de date. Să te bazezi exclusiv pe ratele de modificare a datelor de backup pentru a detecta astfel de comportamente este insuficient și de aceea organizația ta trebuie să poată detecta un atac în timp real.

Este nevoie de o soluție care poate monitoriza și detecta continuu rate de modificare mai mici, analizând fișiere și jurnale de audit - chiar și atunci când nu acorzi o atenție deosebită. Soluția de backup potrivită îți va proteja organizația de atacuri cibernetice la orice moment din zi.

4. Cloud-ul public reprezintă un punct de intrare pentru infracțiunile de tip ransomware

Cloud-ul devine rapid un punct de intrare pentru atacurile cibernetice, ceea ce pune în pericol datele tale de backup. De fapt, McAfee estimează că unul din patru utilizatori de cloud public de astăzi au suferit un furt de date! Concluzia este următoarea: datele din cloud nu sunt imune la atacurile ransomware. Cloud-ul public poate fi rentabil pentru copiile de backup, dar el presupune și o vizibilitate redusă a datelor. Pentru a fi cu un pas înaintea atacurilor ransomware, este nevoie de o soluție de backup și recuperare care să ofere un singur tablou de bord.

Capacitatea de a vedea, gestiona și acționa rapid asupra datelor tale de backup – indiferent că sunt locale sau într-un cloud public – îți va ajuta organizația să se protejeze de atacurile ransomware.

5. Ciclurile lungi de backup și recuperare măresc riscul de atacuri ransomware

Dacă firma ta se bazează pe un backup moștenit care necesită completări sintetice, și este victima unui atac ransomware, echipa ta IT poate petrece zile (chiar săptămâni!) cu recuperarea. Un raport recent al Institutului Ponemon estimează costul mediu al unui singur atac ransomware la 5 milioane de dolari, în principal din cauza pierderii productivității, a timpilor morți ai sistemelor și a furtului de informații. Este nevoie de o soluție de backup și recuperare care să răspundă rapid la atacurile ransomware și care să îți permită să localizezi și să ștergi rapid fișierele infectate de pe amprenta ta globală de date - inclusiv din cloud-urile publice. De asemenea, este nevoie de capacități de restaurare instantanee în masă, care permit recuperarea a sute de mașini virtuale instantaneu, la scară și în orice moment.

Prevenție, detecție și reacție rapidă la atacurile ransomware

Organizații ca a ta doresc să înregistreze zero pierderi de date din atacurile cibernetice și vor să știe cu siguranță că pot refuza cererile de plată de tip ransomware. Protejează-ți datele cu un abonament complet de prevenție, detecție și reacție rapidă la atacurile ransomware.

Contactează echipa noastră pentru a afla mai multe

info@m247.ro +4 031 630 2051 m247.ro