Snabbare återställning efter utpressningstrojaner med Dell PowerProtect-säkerhetskopieringstjänster

Återställ från utpressningstrojaner inom några timmar, inte dagar

Viktiga funktioner

Attacker med utpressningstrojaner blir allt vanligare, mer avancerade och dyrare

- Oförmåga att snabbt identifiera och återställa icke-infekterade säkerhetskopior eller filer
- Spridning av kontaminering och återinfektion från återställningsdata
- Dataförlust, oförmåga att återställa en fullständig datauppsättning
- Svårigheter att samordna orkestrering av åtgärder vid incidenter
- Krav på snabbare RPO-/RTO-tider
- Kostsamma driftavbrott i verksamheten som leder till förlorade intäkter och ryktesskada på varumärket
- Rättsliga och lagstadgade böter på grund av otillräckligt dataskydd

Utmaningen

Utrpressningstrojaner är ett allvarligt hot mot alla företag. Cyberattacker förekommer ofta och kan orsaka katastrofala skador. Inom 79 % av organisationerna finns det en oro för att man upplever en störande händelse under de kommande tolv månaderna1. Företag som förlorar sina data riskerar att gå i konkurs efter en katastrof. Attacker med utpressningstrojaner sker inte bara oftare utan har också blivit mer tekniskt avancerade och dyra.

Lösningen

Snabb och tillförlitlig återställning gör att ingen ens hinner fundera på att betala en lösensumma. Men när en säkerhetsincident eller cyberattack inträffar måste organisationen förstå effekterna och grundorsaken före återställningen. Med en kristallklar ögonblicksbild av arbetsbelastningar och virtuella maskiner som är tillgängliga dygnet runt, kontinuerlig övervakning av användar- och dataavvikelser, integrering med säkerhetsverktyg och automatiserad återställning av rena data kan du förbättra säkerhetsställningen och omvandla en förödande situation till en incident som kan övervinnas.

Möjligheterna

För alla arbetsbelastningar:

• Se till att ha oföränderliga säkerhetskopior med luftfickor tillgängliga dygnet runt.

• Återställ rena data på plats eller i molnet med RPO/RTO på några timmar, inte dagar eller veckor.

• Tjänsten Managed Data Detection and Response (MDDR) ger realtidsövervakning i säkerhetskopieringsmiljöer dygnet runt, året om.

• Att återställa arbetsbelastningar och virtuella datorer inom en AWS-region/ett AWS-konto med hjälp av data från produktionsorganisationen och skapa många kopior av dem som lagras på flera ställen utsätter organisationen för stora risker.

Snabbare återställning vid utpressningstrojaner för viktiga arbetsbelastningar:

• Övervaka och upptäck avvikelser proaktivt med ML-baserade algoritmer.

• Orkestrera svar- och återställningsaktiviteter via SIEM- och SOAR-integreringar.

• Skanna bilder för skadlig kod innan återställning och ta bort infekterade bilder och filer från säkerhetskopior.

• Återställ automatiskt den senaste rena versionen av varje fil inom en viss tidsram från en gyllene ögonblicksbild.

Skydd

Det första steget för att förhindra skador från utpressningstrojaner är att se till att du har oföränderlig kopia av dina data med luftfickor. PowerProtect-säkerhetskopieringstjänster bygger på en mycket motståndskraftig molninfrastruktur och gör det omöjligt för utpressningstrojaner att kryptera säkerhetskopieringsdata. Nollförtroendearkitektur, inklusive flerfaktorsautentisering, kryptering av kuvert och separat kontoåtkomst säkerställer att utpressningstrojaner inte kan använda komprometterade inloggningsuppgifter för den primära miljön i syfte att manipulera säkerhetskopieringsmiljön eller data. Slutligen ger funktioner för att förhindra att du tar bort stora mängder och mjuk borttagning (Papperskorgen) ytterligare ett säkerhetslager för att skydda säkerhetskopior mot radering.

Identifiering

Att upptäcka en attack med en utpressningstrojan så snart som möjligt kan hjälpa incidentsvarsteamen och förhindra att kontaminationen sprids. Dell PowerProtect-säkerhetskopieringstjänsternas accelererade återställningsmodul för utpressningstrojaner ger ett säkerhetscenter för att övervaka statusen för din säkerhetskopieringsmiljö. Med åtkomstinsikter och avvikelsedetektering kan du snabbt identifiera ovanliga aktiviteter i din miljö och bland dina data. Se information om plats, identitet och aktivitet för alla åtkomstförsök från användare och API:er. Upptäck avvikelser med tillverkarspecifika ML-algoritmer som ger varningar vid ovanlig dataaktivitet (t.ex. radering, kryptering osv.). Algoritmen lär sig mönster för din specifika säkerhetskopieringsmiljö, så det krävs inga regelinställningar eller några finjusteringar. Den använder även entropibaserade insikter för att minska falska positiva resultat

Svar

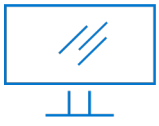
När en säkerhets- eller it-analytiker upptäcker en misstänkt händelse, eller ännu värre, bekräftar att en incident med en utpressningstrojan har ägt rum, blir svarstiden kritisk. Även om det finns många värdefulla primära miljösäkerhetsverktyg som kan användas för detektering och responsorkestrering, förbättrar analyser och ändringar av loggdata från sekundära data (säkerhetskopieringssystem) aktiviteter för utredning och respons samt forensiska aktiviteter. Dells PowerProtect-säkerhetskopieringstjänster har en accelererad återställningsmodul för utpressningstrojaner som erbjuder robusta API-integreringar direkt vid leverans och gör det enkelt att passa in lösningen i ditt övergripande säkerhetsekosystem. Orkestrering av svarsaktiviteter med SIEM- och SOAR-lösningar kan dramatiskt minska din genomsnittliga tid att svara (MTTR) genom att automatiskt slutföra åtgärder som att sätta infekterade system eller ögonblicksbilder i karantän eller skanna säkerhetskopior för IOC:er baserat på en förutbestämd playbook för utpressningstrojaner.

Återvinning

Efter den första svarsfasen kommer det hårda arbetet med återställning. För många företag är detta en manuell och tidskrävande process. Kvardröjningstiden för skadliga aktörer och utpressningstrojaner kan sträcka sig från veckor till månader, vilket gör det svårt att veta hur långt tillbaka man ska gå för att hitta rena data. Även när den bästa ögonblicksbilden har identifierats kan dolda skadliga program orsaka återinfektion. Men en återställningspunkt för två veckor sedan är inte acceptabel för de flesta företagsanvändare. Men att hitta och validera nyare data efter en incident med en utpressningstrojan är manuellt, tråkigt och ofta praktiskt omöjligt.

Dell PowerProtect-säkerhetskopieringstjänsterna förenklar arbetet med en effektiv säkerhetskopieringsarkitektur och automatiserade verktyg för att påskynda återställningen. Molnplattformen med Dell PowerProtect-säkerhetskopieringstjänster säkerhetskopierar arbetsbelastningar direkt till molnet, redo för omedelbar återställning i händelse av en attack med utpressningstrojaner.

Den accelererade återställningsmodulen för utpressningstrojaner gör att du tryggt kan återställa genom att säkerställa hygienen hos återställningsdata. Du kan skanna ögonblicksbilder efter skadliga program och IOC med hjälp av inbyggd antivirusdetektering eller med hjälp av hotinformation från dina egna forensiska undersökningar eller informationsflöden om hot. Att skanna bilder innan återställning eliminerar återinfektion.



Mer information om PowerProtect-säkerhetskopieringstjänster

Kontakt en av Dell Technologies experter