DELL Technologies

Utpressningsvirus: Stärk cybersäkerheten och motståndskraften med Dell Technologies

Vad är utpressningsvirus?

Utpressningsvirus är en typ av skadlig programvara som blockerar åtkomst till ett datorsystem eller data tills en lösensumma betalas. Det är en av de cyberattacker som orsakar mest störningar. Hälften av alla företag globalt har under det senaste året drabbats av en utpressningsvirusattack minst en gång, och i genomsnitt varar driftstoppet efter en attack i tre veckor. Resultatet är stora störningar i verksamheten.

Ökande hot om utpressningsvirus

Utpressningsvirus är en typ av skadlig programvara som blockerar åtkomst till ett datorsystem eller data tills en lösensumma betalas. Det är en av de cyberattacker som orsakar mest störningar. Hälften av alla företag globalt har under det senaste året drabbats av en utpressningsvirusattack minst en gång, och i genomsnitt varar driftstoppet efter en attack i tre veckor. Resultatet är stora störningar i verksamheten.

Så fungerar utpressningsvirus

Utpressningsvirus infekterar vanligtvis företagets system när någon klickar på en skadlig länk, öppnar en infekterad bilaga eller besöker en komprometterad webbplats. Viruset tar sig sedan in i system för att kryptera filer, och gör dem oläsliga. Då visar utpressningsvirusprogrammet ett meddelande om att betalning krävs (ofta i kryptovaluta) i utbyte mot en dekrypteringsnyckel. Om lösensumman inte betalas kan angriparen hota att radera data eller läcka dem offentligt. Ett vanligt exempel på en utpressningsvirusattack som kom 2017 var WannaCry-attacken. Den spred sig snabbt över hela världen och påverkade sjukhus, företag och myndigheter och hade en enorm ekonomisk inverkan. Den globala ekonomiska effekten av WannaCry-viruset var mellan 4 till 8 miljarder USD enligt Cyber Risk Management (CyRiM) och Lloyd's of London och över 200 000 system påverkades i 150 länder inom bara några dagar.

Två av världens största företag som påverkades var FedEx, som rapporterade en förlust på 300 miljoner USD på grund av störningar och sanering, och Renault-Nissan som var tvungna att tillfälligt stoppa produktionen i flera fabriker. De dolda kostnaderna efter en utpressningsvirusattack kan vara många, bland annat:

- Driftavbrott i företaget och förlorad produktivitet
- Skadat anseende
- Kostnad för systemåterställning och korrigering
- Juridiska och lagstadgade böter

När företag drabbas av en utpressningsvirusattack bör de vidta följande steg:

- Betala inte om det inte är absolut nödvändigt – det finns ingen garanti för att angriparna återställer åtkomst.
- Återställ från säkerhetskopior om det är möjligt.
- Rapportera attacken till myndigheterna.
- Stärk försvaret för att förhindra framtida angrepp (exempelvis hålla mjukvaran uppdaterad, utbilda personal, använda slutpunktsskydd).

Bekämpa utpressningsvirusattacker med Dell Technologies

Dell Technologies utrustar företag med omfattande och framtidssäkra verktyg som utformats för att förhindra risker med utpressningsvirusattacker innan de orsakar skada.

Förbättrad slutpunktssäkerhet med Dell Trusted Devices

Slutpunkter är ofta de primära ingångspunkterna för utpressningsvirusattacker och gör slutpunktssäkerhet till ett viktigt fokusområde. Dell Trusted Devices integrerar hårdvaruaktiverade säkerhetsfunktioner som skyddar system utan att kompromissa med prestanda. Lösningar som Dell SafeBIOS och SafeID stärker slutpunktsenheter mot obehörig åtkomst, medan Dell SafeData krypterar data för att skydda känslig information även utanför företagets brandvägg. Genom att bygga in säkerhet i själva enheterna kan företag skydda sig på hårdvarunivå, vilket minskar risken för att angripare får fotfäste.

Proaktiv övervakning med CrowdStrike

Utpressningsvirusattacker är inte oundvikliga om företag använder rätt verktyg för att upptäcka och reagera på hot i realtid. CrowdStrike, som erbjuds som en del av Dells lösningsportfölj, erbjuder nästa generations plattform för slutpunktsskydd som drivs av AI och beteendeanalys. Den här tekniken identifierar och neutraliserar misstänkt aktivitet innan den utvecklas till en attack. CrowdStrike integreras smidigt med Dells infrastruktur och gör det möjligt för IT-teamen att upprätthålla synlighet i hela miljön, vilket ger omedelbar och effektiv hotrespons.

Omfattande dataskydd med Dell PowerProtect

Dell PowerProtect-lösningar är avgörande för att stå emot utpressningsvirus. Dessa avancerade dataskyddsverktyg är utformade för att skydda företagsdata mot både interna och externa hot. Funktioner som oföränderliga säkerhetskopior säkerställer att dina data inte kan ändras, raderas eller krypteras av utpressningsvirus. Det ger ett tillförlitligt säkerhetsnät även vid avancerade attacker. Dell PowerProtect Cyber Recovery Vault isolerar till exempel kritiska data från nätverket med luftgapteknik. Det säkerställer att de förblir oförändrade även under de mest sofistikerade intrången. Med automatiserad avvikelsedetektering och smarta arbetsflöden får organisationer möjlighet att upptäcka skadlig aktivitet tidigt och reagera innan utpressningsvirus sprids.

Avancerad nätverkssäkerhet och mikrosegmentering med Dell PowerSwitch Networking och SmartFabric OS

Stärker försvaret mot nolldagsattacker genom att leverera avancerad nätverkssegmentering, strikta åtkomstkontroller och trafikanalys i realtid i hela infrastrukturen.

Återställning i stor skala med Dell Data Protection Services

Dell inser att även om förebyggande åtgärder är avgörande, är återhämtning en lika viktig del av beredskapen mot utpressningsvirus. Dell Data Protection Services tillhandahåller inte bara automatiserade säkerhetskopierings- och återställningslösningar utan även expertledd rådgivning för att säkerställa att företag kan återhämta sig snabbt och minimera driftavbrott. Tjänster som fjärrdataräddning och incidenthantering säkerställer att företag har den support de behöver under kritiska situationer. Denna helhetsstrategi garanterar att dataintegriteten bevaras och att återhämtning sker snabbare, vilket minskar driftstörningar.

Det här är bara några exempel i Dells portfölj med lösningar som kan hjälpa till med skadliga insiderhot.

Starka genom samarbeten

Dells samarbetsstrategi utökar skyddet bortom Dells teknik. Genom partnerskap med ledande cybersäkerhetsföretag som CrowdStrike och Secureworks erbjuder Dell ett ekosystem av integrerade lösningar som hanterar alla möjliga attackvektorer. Tillsammans ger dessa lösningar heltäckande säkerhet och gör det möjligt för företag att skapa försvar i flera lager som är skräddarsydda för deras unika riskprofiler.

Varför välja Dell?

Dell Technologies är mer än en teknikleverantör – det är en betrodd partner i kampen mot utpressningsvirus. Genom att kombinera innovation, expertis och engagemang för att stärka företag ger Dell företag de verktyg och den trygghet som krävs för att möta föränderliga hot. Dells produkter och tjänster säkerställer driftskontinuitet och ger sinnesro, oavsett om det handlar om att skydda slutpunkter, skydda kritiska data eller möjliggöra snabb återställning.

Bygg en motståndskraftig framtid

Utpressningsvirusattacker fortsätter att utvecklas men med Dell Technologies kan företag ligga steget före. Genom att utnyttja avancerad hårdvara, mjukvara och tjänster kan företag bygga ett ramverk för cybersäkerhet som är tåligt, anpassningsbart och tillförlitligt. Skydda dina data, din verksamhet och framtidssäkra ditt företag idag med Dells omfattande lösningar mot utpressningsvirus.

För att stärka företagets motståndskraft är det viktigt att känna till de aktuella hoten och vara informerad om nya hot som dyker upp. Dell Technologies cybersäkerhetsexperter övervakar ständigt nya attackvektorer och arbetar för att proaktivt åtgärda potentiella sårbarheter i våra produkter och tjänster. Detta gör att vi kan ge dig det mest uppdaterade skyddet mot ständigt föränderliga hot av utpressningsvirus.

Utöver att hålla sig informerade måste företag också påbörja en säkerhetsstrategi i flera lager. Det innebär att installera en rad säkerhetsåtgärder: brandväggar, mjukvara för skydd mot skadliga program, intrångsdetekteringssystem och säkerhetskopiering av data. Genom att diversifiera dina försvarsstrategier kan du minimera effekten av en attack och se till att ditt företag förblir i drift även om ett framgångsrikt utpressningsförsök har genomförts.

Det är också viktigt att regelbundet testa och uppdatera dina säkerhetsåtgärder (både korrigera dina system och uppdatera dina policyer). Hackare hittar ständigt nya sätt att kringgå traditionella säkerhetsåtgärder, så det är viktigt att företagen ligger steget före genom att regelbundet testa sina försvar och uppdatera dem efter behov. Detta inkluderar regelbundna sårbarhetsbedömningar, intrångstestning och korrigeringshantering.

En annan viktig aspekt för att skydda ditt företag mot utpressningsvirus är att utbilda medarbetarna om bästa metoderna för cybersäkerhet. Många utpressningsvirusattacker initieras genom taktiker för socialteknik, till exempel nätfiskemejl eller skadliga länkar. Genom att utbilda dina medarbetare om hur du upptäcker och undviker dessa hot kan du avsevärt minska sannolikheten för en attack sker.

Skapa även en katastrofåterställningsplan, det kan avsevärt minska effekten av en utpressningsvirusattack. Planen bör omfatta regelbundna säkerhetskopieringar av viktiga data och system, samt en tydlig procedur för att svara på attacker och återställning.

Utöver dessa proaktiva åtgärder är det också viktigt att ha en stark incidenthanteringsplan på plats. Detta inkluderar tydligt definierade roller och ansvar för att hantera en utpressningsvirusattack samt kommunikationsprotokoll för att meddela intressenter och mildra skador.

Slutligen kan du ligga steget före potentiella hot genom att hålla dig informerad om de senaste trenderna och utvecklingen inom utpressningsvirusattacker. Genom att regelbundet granska branschrapporter och uppdateringar från säkerhetsexperter kan du proaktivt implementera nya säkerhetsåtgärder för att skydda ditt företag.

Kom ihåg att inget företag är immunt mot utpressningsvirusattacker men med rätt strategier och verktyg på plats kan du minimera risken för och effekten av sådana attacker. Genom att ha en proaktiv strategi för cybersäkerhet skyddar du inte bara ditt företag utan bygger också upp förtroende hos dina kunder och intressenter.

Lär dig att hantera några av dagens främsta cybersäkerhetsutmaningar på **Dell.com/SecuritySolutions**

Mer information om Dells lösningar

Kontakta en av Dell Technologies experter

Visa fler resurser

Delta i samtalet med #HashTag

DELL Technologies