Kratak pregled rešenja

Dell PowerProtect Cyber Recovery

Savremena i otporna zaštita važnih podataka od destruktivnih sajber napada i ransomvera (ransomware)

ČEMU SLUŽI OPORAVAK OD SAJBER NAPADA?

Sajber napadi imaju za cilj da unište, ukradu ili na drugi način kompromituju vaše osetljive podatke – uključujući i rezervne kopije. Zaštita važnih podataka i obezbeđivanje njihovog integriteta tokom oporavka su ključni faktori za nastavak redovnih poslovnih operacija nakon napada. Da li bi vaša kompanija mogla to da izdrži? Ovo su elementi rešenja koje vam nudi otpornost na sajber napad:

Izolacija podataka i upravljanje

Postavka udaljenog centra podataka koji nije deo korporativnih i rezervnih mreža i koji je dostupan samo za korisnike uz odgovarajuću dozvolu.

Automatsko kopiranje podataka i air-gap izolacija mreža

Kreiranje nepromenljivih kopija podataka u bezbednom digitalnom trezoru i procesi koji stvaraju operativnu air-gap izolaciju mreža između proizvodnog/rezervnog okruženja i trezora.

Inteligentna analitika i alati

Mašinsko učenje i indeksiranje punog sadržaja uz moćnu analitiku u okviru bezbednosti trezora. Automatske provere integriteta služe da bi se utvrdilo da li je malver imao uticaj na podatke i ukoliko je potrebno koriste se alati kao pomoć u sanaciji.

Oporavak i sanacija

Tokovi poslovanja i primena alata za oporavak nakon incidenta uz dinamičke procese vraćanja podataka i postojeće DR procedure.

Planiranje i projektovanje rešenja

Uz ekspertsku pomoć, odabir kritičnih skupova podataka, aplikacija i drugih ključnih sredstava za određivanje vremena potrebnog za oporavak i maksimalnog vremena za toleranciju i pojednostavljenje oporavka.

Izazov: Sajber napadi su neprijatelj preduzeća čije se poslovanje zasniva na upravljanju podacima

Podaci su valuta internet ekonomije, te su samim tim i vitalni resurs koji mora biti zaštićen, poverljiv i dostupan u svakom trenutku. Današnje globalno tržište oslanja se na kontinuirani protok podataka kroz međusobno povezane mreže, dok napori implementacije digitalnih transformacija dovode osetljivije podatke u opasnost. Zbog toga, za sajber kriminalce, podaci u vašoj kompaniji su unosna i atraktivna meta. Bez obzira na privrednu granu ili veličinu organizacije, preduzeća i državne ustanove su konstantno izloženi riziku od sajber napada, njihovi podaci su kompromitovani, a često se sreću i sa smanjenim prihodom zbog zastoja u poslovanju, lošom reputacijom i skupim regulatornim kaznama. Strategija sajber otpornosti postaje obavezna za rukovodioce u preduzećima i državnim institucijama, međutim, mnoge organizacije nemaju poverenja u dostupna rešenja za zaštitu podataka. Prema Globalnom indeksu zaštite podataka, 79% donosilaca odluka u IT sektoru se plaši da će doći do neželjenog događaja u narednoj godini, dok 75% iskazuje zabrinutost da postojeće mere zaštite podataka u njihovim kompanijama neće biti dovoljne da se nose sa pretnjama od malvera (malwera) i ransomvera.

Koje korake možete preduzeti da biste zaštitili svoju kompaniju, klijente, osoblje i osetljive podatke?

Rešenje: Dell PowerProtect Cyber Recovery

Da biste smanjili rizik poslovanja izazvan sajber napadima i da biste omogućili zaštitu podataka koja je otpornija na sajber napade, možete da modernizujete i automatizujete strategije oporavka i obezbedite kontinuitet poslovanja tako što ćete koristiti najnovije inteligentne alate za otkrivanje i odbranu od sajber pretnji.

Dell PowerProtect Cyber Recovery pruža testiranu, najsavremeniju, otpornu i inteligentnu zaštitu za izolovanje važnih podataka, uočavanje sumnjivih aktivnosti i brži oporavak podataka omogućavajući vam da brzo nastavite sa normalnim poslovnim operacijama.

PowerProtect Cyber Recovery – Nepromenljivost, izolacija i inteligencija

Cyber Recovery trezor

Trezor u okviru PowerProtect Cyber Recovery nudi više slojeva zaštite za povećanje otpornosti od sajber napada, uključujući i pretnje koje dolaze iznutra. Ovaj sistem fizički izoluje podatke unutar bezbednog područja centra podataka, udaljavajući ih od potencijalnih tačaka napada. Pristup podacima se odobrava preko više slojeva autentifikacije i jedinstvenih bezbednosnih akreditiva. Dodatne mere zaštite uključuju automatizovani operativni air gap sistem koji obezbeđuje izolaciju mreže i eliminiše potencijalno ugrožene interfejse za upravljanje. PowerProtect Cyber Recovery automatizuje sinhronizaciju podataka između proizvodnih sistema, uključujući otvorene sisteme i glavne računare i trezora, čime se stvaraju nepromenjene kopije za koje važi politika zadržavanja rezervnih kopija. Ukoliko dođe do sajber napada, možete brzo identifikovati čistu kopiju podataka, oporaviti osetljive sisteme i ponovo pokrenuti svoje poslovanje.

CyberSense

PowerProtect Cyber Recovery je prvo rešenje koje u potpunosti integriše CyberSense, čime se dodaje inteligentni sloj zaštite koji pomaže u otkrivanju oštećenja podataka kada napad uđe u centar podataka. Ovaj inovativni pristup uključuje potpuno indeksiranje sadržaja i koristi mašinsko učenje zasnovano na veštačkoj inteligenciji za analizu preko 200 statističkih podataka zasnovanih na sadržaju i otkrivanje znakova neispravnosti koji nastaju kao posledica ransomvera. CyberSense otkriva nepravilnost sa do 99,5% pouzdanosti, pomažući vam da identifikujete pretnje i dijagnostikujete vektore napada, istovremeno štiteći sadržaj koji vam je jako važan za poslovanje – sve u okviru delokruga bezbednosnog trezora.

Oporavak i sanacija

PowerProtect Cyber Recovery nudi automatizovane procese oporavka i obnavljanja za bezbedno i pouzdano vraćanje osetljivih sistema u okviru poslovanja na mrežu. Oporavak je integrisan sa vašim procesom reagovanja na incident. Nakon što dođe do incidenta, tim za reagovanje na incident analizira proizvodno okruženje kako bi utvrdio primarni uzrok tog događaja. CyberSense takođe omogućava izradu forenzičkih izveštaja nakon napada koji pomažu u određivanju obima i dubine napada i pruža listu poslednjih pouzdanih rezervnih skupova pre neispravnosti. Nakon toga, kada je proizvodnja spremna za oporavak, Cyber Recovery obezbeđuje alate za upravljanje i tehnologiju koja obavlja stvarni oporavak podataka. To automatizuje kreiranje tačaka vraćanja koje se koriste za oporavak ili bezbednosnu analitiku.

Planiranje i projektovanje rešenja

Opcione Dell Advisory (savetodavne) usluge vam pomažu da odredite koje osetljive sisteme u poslovanju treba da zaštitite, kao i da kreirate mape međuzavisnosti za povezane aplikacije i usluge i infrastrukturu potrebnu za njihov oporavak. Usluga takođe generiše zahteve za oporavak i alternative dizajna i identifikuje tehnologije za analizu, hostovanje i zaštitu vaših podataka, zajedno sa vremenskom linijom implementacije poslovanja.

ZA ZAŠTITU VAŠIH VAŽNIH PODATAKA OD SAJBER NAPADA NEOPHODNO JE DA KORISTITE POZNATA, SAVREMENA I OTPORNA REŠENJA. POWERPROTECT CYBER RECOVERY VAM PRUŽA SIGURNOST DA MOŽETE BRZO DA IDENTIFIKUJETE I VRATITE POZNATE ZNAČAJNE PODATKE I NASTAVITE SA NORMALNIM POSLOVANJEM NAKON SAJBER NAPADA.

Saznaj više o Dell PowerProtect Cyber Recovery	Kontaktirajte predstavnika prodaje PROINTER-WEB na office@prointerweb.rs	Više o Dell bezbednosnim rešenjima	PROINTER Web