datto

RANSOMWARE PROTECTION & RECOVERY SOLUTION (RPRS)

Solution Sheet

Uw data is waardevoller voor u dan voor iemand anders. Dat is waarom hackers achter uw data aanzitten: zodat ze die aan u terug kunnen verkopen. Ze willen uw bedrijf gijzelen voor losgeld. Een werknemer hoeft slechts één keer te klikken op een bijlage in een e-mail die gepersonaliseerd en ontworpen is om echt te lijken. Die ene klik start een proces waarbij de bestanden van die werknemer worden vergrendeld. Vervolgens verspreidt het zich naar andere desktops en servers op het netwerk. Als er niets wordt gedaan, ligt uw bedrijf binnen enkele uren plat. Uw waardevolle data wordt versleuteld en gemarkeerd voor verwijdering, tenzij het losgeld wordt betaald. De meeste aanvallen bevatten ook een aftelklok waarbij stukjes van uw bedrijfsdata permanent worden verwijderd terwijl de klok doortikt en er geen losgeld wordt betaald.

Als dit u of een klant van u weleens is overkomen, dan bent u niet alleen. Ransomwareaanvallen komen op ongekende schaal voor. Terwijl individuele aanvallen bedragen opleveren van een paar honderd tot duizenden dollars, bracht ransomware ruim 325 miljoen dollar op in 2015 en al ruim 200 miljoen dollar in de eerste helft van 2016. Maar wat kunt u er vandaag de dag tegen doen?

RANSOMWARE BRACHT RUIM 325 MILJOEN DOLLAR OP IN 2015 EN AL 200 MILJOEN DOLLAR IN DE EERSTE HELFT VAN 2016

Ransomware Protection & Recovery Solution

Datto is verheugd om de eerste Ransomware Protection & Recovery Solution (RPRS) in de sector aan te kondigen. Gebaseerd op innovatieve nieuwe functies in de productlijnen van Datto SIRIS, NAS, Backupify en Datto Drive, detecteert deze oplossing een ransomwareaanval en zet ze systemen terug naar een tijdstip voorafgaand aan de aanval. Zo worden onder andere bestanden en mappen op het gehele netwerk beschermd, evenals op mobiele apparaten, werkstations en in de cloud.

Zo profiteert u van de voordelen van RPRS:

1. Wees er zeker van dat uw systemen en bestanden zo snel mogelijk worden beschermd door het SIRIS 3 Total Data Protection-platform en is voor alle fysieke en virtuele systemen in te zetten. Stel een regelmatig back-upschema in.
2. Identificeer aanvullende back-upbehoeften op het netwerk, op mobiele apparaten en in de cloud. Maak er back-ups van met Datto NAS, Datto Drive en Datto Backupify.
3. Wanneer een ransomwareaanval start, wordt het aanvalsprofiel snel gedetecteerd en zal een beheerder worden ingelicht.
4. De beheerder herstelt het getroffen systeem naar een snapshot van vóór de aanval. Hierdoor wordt de aanval verwijderd.
5. In het geval van infectie worden de bestandsopslag van het netwerk, van mobiele apparaten en bestanden in de cloud hersteld zoals noodzakelijk om te voorkomen dat restanten van de ransomware een nieuwe infectie kunnen vormen.
6. Het bedrijf hervat de werkzaamheden zoals gewoonlijk. Er wordt geen losgeld betaald en er zijn geen bestanden verloren gegaan. Er is slechts een korte onderbreking. In enkele minuten is alles voorbij.

U HEBT EEN MANIER NODIG OM DEZE AANVALLEN SNEL TE DETECTEREN EN ERVAN TE HERSTELLEN – IETS WAT DEZE BESTAANDE TECHNOLOGIEËN MISSEN. U HEBT RPRS NODIG

Zoals met de meeste disaster recovery-scenario's is plannen en voorbereiden de beste aanpak. Hoewel voorlichting van de eindgebruikers en endpoint & perimeter protection solutions belangrijke onderdelen van zo'n plan zijn, zijn ze niet voldoende. De meeste bedrijven gebruiken deze oplossingen al, maar er komt nog steeds ransomware doorheen. Om uw bedrijf grondig te beschermen, hebt u meer nodig dan white- en blacklists. U hebt een manier nodig om deze aanvallen snel te detecteren en ervan te herstellen – iets wat deze bestaande technologieën missen. U hebt RPRS nodig.

De Ransomware Protection & Recovery Solution is een verzameling van gecombineerde Datto-producten om bedrijven te beschermen tegen de gevolgen van ransomwareaanvallen. De oplossing bevat SIRIS 3-detectie, back-up- en herstelmogelijkheden, evenals NAS 3, Backupify en Datto Drive om – waar dan ook – bedrijfsdata te beschermen tegen ransomware.

SIRIS 3

De enige, zekere manier om een ransomwareaanval op te lossen, is om de geïnfecteerde systemen te herstellen en zo effectief de klok terug te draaien. SIRIS 3 – met ransomwaredetectie en het terugzetten naar een herstelpunt – is ontworpen om een aanval te identificeren, beheerders in te lichten en van deze scenario's te herstellen. Binnen enkele minuten is het alsof de ransomwareaanval nooit heeft plaatsgevonden. Zet ransomware en andere rampen buiten de deur en haal eenvoudige preventieve maatregelen van SIRIS binnen.

Backupify

Er wordt vaak van ransomware gedacht dat het alleen een bedreiging ter plaatse vormt, maar niets is minder waar. Hoe hard u het ook probeert tegen te houden, iemands computer zal geïnfecteerd raken met ransomware. Als de gebruiker bestanden synct met Google Drive of OneDrive, zal ransomware ook bestanden in de cloud versleutelen. Verhelp ransomware met de SaaS-back-upoplossing en herstel eenvoudig naar een tijdstip voorafgaand aan de versleuteling van uw bestanden.

Datto NAS 3

Ransomware is niet alleen een probleem voor endpoint- en serversystemen, maar het treft ook alle data die op het netwerk is opgeslagen. Ons netwerkverbonden opslagproduct NAS 3 (Network-Attached Storage) met NAS Guard kan al uw netwerkopslagapparaten opslaan en automatisch data inplannen en kopiëren naar de lokale Datto NAS. Van deze data wordt een back-up gemaakt in de beveiligde Datto Cloud – klaar om, wanneer dan ook, als herstelpunt gebruikt te worden. Bescherm uw bestaande netwerkopslag tegen ransomwareaanvallen met NAS Guard.

Datto Drive

Traditionele oplossingen voor het synchroniseren en delen van bestanden zijn zeer gevoelig voor ransomwareaanvallen. Als één computer simpelweg geïnfecteerd raakt, worden bestanden vervolgens automatisch gesynchroniseerd op alle apparaten – inclusief mobiel. Datto Drive is het enige platform dat standaard beschermt tegen ransomware door volledige back-ups van alle bestanden op het platform voor synchroniseren en delen te maken. Hierdoor wordt het mogelijk naar een herstelpunt te gaan voorafgaand aan een incident. Met Datto Drive verwijdert u de gevolgen van ransomware bij het synchroniseren en delen van bestanden.

Ga voor meer informatie over ransomware naar www.datto.com/ransomware.

datto

Corporate Headquarters
Datto, Inc.
101 Merritt 7
Norwalk, CT 06851
United States
partners@datto.com
www.datto.com
888.294.6312

Datto EMEA
250 Longwater Avenue, Green Park
Reading RG2 6GB
United Kingdom
+44 (0) 118 402 9606

Global Offices
USA: 888.294.6312
Canada: 877.811.0577
EMEA: +44 (0) 118 402 9606
Australia: +61 406 504 556
Singapore: +65-31586291