ADVERTORIAL

Uw bedrijfskritische data beschermen

Iedere dag worden bedrijven, instellingen of particulieren geraakt door ransomware of malware. Het is vandaag de dag helaas niet meer de vraag of je gehackt wordt maar eerder wanneer; het gebeurt al vaak zonder dat we het door hebben. Uit een rapport van het Nationaal Cyber Security Centrum bleek dat er wereldwijd 1800 bedrijven zijn getroffen door gijzelsoftware. Een aantal daarvan ook in Nederland.

Hebben we het over ransomware dan wordt er vaak relatief weinig 'losgeld' gevraagd. Daarmee is dit dan ook slechts een klein deel van de werkelijke totale kosten van zo'n aanval. Zonder data geen bedrijfsvoering; de gevolgen van zo'n incident kunnen echter wel desastreus zijn voor uw organisatie. Denk hierbij aan verlies van data, omzet en mogelijke reputatieschade wat weer kan leiden tot een vertrouwensbreuk met uw klanten. Ook wordt veelal na het betalen van het losgeld niet de benodigde decryptie software gegeven en is de kans groot dat na verloop van tijd er een tweede aanval zal worden gedaan. De aanvaller weet immers dat er hoogstwaarschijnlijk weer zal worden betaald...

Het beschermen tegen cyber attacks ofwel uw cyber resilience kent verschillende lagen. Van goed naar beter naar best. Het is goed om data veilig te stellen met een back-up op disk of tape en herhaaldelijk het herstel te testen. Maar kwaadwillenden hebben steeds vaker het doel om naast primaire data ook back-up data te vernietigen of te versleutelen. De beste en ook veiligste oplossing is een onveranderbare kopie van back-up data en catalogus in een onzichtbare kluis te stoppen. Deze onzichtbare kluis, ook wel een cyber recovery vault genoemd, is zowel fysiek, als qua productie netwerk connectiviteit afgesloten van de productie omgeving. Het verbergen van data in een kluis is de juiste aanpak, maar niet de oplossing voor alles. Anders zou een tape ook voldoen. De opgeslagen data moet ook continu geanalyseerd worden op verdachte veranderingen die duiden op malware of ransomware. Want wanneer weet u dat data geïnfecteerd is?

Hiervoor wordt met cyber recovery software de data in de kluis automatisch geanalyseerd op verdachte veranderingen zoals aangepaste file extensies, bestandsgrootte, corrupte file structuur, corrupte file content of deels versleutelde bestandsinhoud. Vervolgens wordt hier direct over gerapporteerd. Met deze aanpak kan nog niet eerder geïdentificeerde malware of ransomware worden gedetecteerd. Het is mogelijk om binnen de kluis in een zogenaamde 'clean-room' de data te controleren zonder invloed van buiten en daarna getroffen productiesystemen te herstellen. Onze teams en onze specialisten gaan vanzelfsprekend graag met u in gesprek over onze oplossingen die bijdragen aan uw cyber resilience.

Jean Jacques Kroesbergen
Director Public & Connected Sustainable Society by **Dell Technologies Nederland**.

U kunt mij bereiken via mail
Jean_Jacques_Kroesbe@Dell.com
of bel naar **+31615629320**

DELL Technologies