

Success Story | Data back-up | Silent Bricks

Gemeente Vaals

Moderne ransomware-hackers maken tegenwoordig eerst de back-ups met data onbruikbaar, voordat de schadelijke software geactiveerd en de waardevolle data versleuteld worden. Zo ook bij meerdere Nederlandse gemeentes. Reden genoeg voor de Vereniging van Nederlandse Gemeentes om het advies uit te brengen ook een kopie van de back-up buiten het bereik van de hackers te hebben.

De gemeente Vaals zocht een betrouwbare oplossing voor deze air-gap functionaliteit die de nadelen van een tape-gebaseerd back-up oplost en ook een snelle restore vanuit dit extra beveiligde back-up biedt. Idealiter moest de oplossing gecertificeerd zijn voor de door de gemeente Vaals gebruikte Veeam back-up software.



“Als gemeente Vaals investeren we veel tijd en geld in opleiding van medewerkers om digitale bedreigingen buiten de deur te houden, maar dat is nog geen garantie dat dat werkelijk succesvol is. Zelfs de meest geavanceerde bedrijven worden gehackt, dan moeten we als gemeente Vaals niet de illusie hebben dat we slim genoeg zijn om hackers buiten te houden.”

Erik Winands – systeem- en netwerkbeheerder, gemeente Vaals

Alle foto's:

Gemeente Vaals |

Augustus 2022

Silent Bricks voor de gemeente Vaals:

Een goede back-up die voor hackers onbereikbaar is

Bedrijven en organisaties zijn steeds vaker het doelwit van hackers, die met ransomware het complete netwerk plat kunnen leggen. Ook gemeenten zijn het slachtoffer geworden van ransomware, reden waarom de gemeente Vaals oplossingen zocht om data veilig te bewaren. Een extra uitdaging was dat de oplossing in de bestaande Veeam back-up infrastructuur geïntegreerd werd.

Gemeenten en andere (semi-)overheidsinstellingen zijn momenteel een gewild doelwit voor hackers, die na een hack vaak ransomware of andere malware installeren. Daarmee worden de data versleuteld en die worden pas weer vrijgegeven na het betalen van losgeld. Als het meezit. Al met al levert ransomware veel schade op. Het is begrijpelijk dat de Vereniging van Nederlandse Gemeenten (VNG) daarom alle leden waarschuwde voor dergelijke cyberaanvallen en aandrang op maatregelen. Erik Winands is systeem- en netwerkbeheerder bij de gemeente Vaals. Ook de gemeente Vaals liep tegen de digitale bedreiging en daarmee uitdaging aan die de VNG voorschotelde. “We hadden uiteraard een back-upstelsel met Veeam back-up software, maar vroegen ons daarnaast af hoe we nog iets extra’s kunnen doen zodat we ook veilig zijn als het hele netwerk een keer platligt door een cyberaanval.”

Een laatste reddingsboei

Erik daarover: “Je wilt altijd de garantie hebben dat als iemand door al je veiligheidsmaatregelen breekt, dat je dan nog een laatste reddingsboei hebt qua data, waarmee je je netwerkomgeving weer kan opbouwen. Als gemeente Vaals investeren we veel tijd en geld in opleiding van medewerkers om digitale bedreigingen buiten de deur te houden, maar dat is nog geen garantie dat dat werkelijk succesvol is. Zelfs de meest

geavanceerde bedrijven worden gehackt, dan moeten we als gemeente Vaals niet de illusie hebben dat we slim genoeg zijn om hackers buiten te houden.”

Andere aanpak

Erik ziet dat veel collega-gemeenten druk zijn met maatregelen om hackers vooral buiten de deur te houden. De gemeente Vaals pakte het anders aan. “We wilden zeker weten dat als we door malware worden getroffen, dat we ergens op konden terugvallen. Dus: zorgen voor een goede back-up die voor hackers onbereikbaar is. Dan heb je op het moment dat je gehackt bent in ieder geval nog de beschikking over data waarmee je terug kunt naar de situatie zoals je die wilt hebben. Dat hebben we nu gecreëerd en dat is voor de gemeente Vaals een grote geruststelling. Hackers spelen een kat-en-muisspel en ze hoeven maar één keer raak te schieten, waar wij onze beveiliging altijd op 100 procent moeten hebben. Natuurlijk moet je ervoor zorgen dat je het een hacker moeilijk maakt om binnen te komen en dat je alle maatregelen neemt met geavanceerde beveiligingstechnieken, maar daarnaast is het zaak om te zorgen voor een back-up die voor hackers onbereikbaar is.”





Automatische replicatie

Erik: “Je moet er dus altijd voor zorgen dat je ergens een back-up in de kluis hebt liggen. Dus dan ga je denken aan externe harde schijven of tapes, maar dat zijn zeer arbeidsintensieve oplossingen. COMEX is gespecialiseerd in alternatieve oplossingen voor dit vraagstuk en is bovendien in de gemeente opgericht en nog altijd in de regio gevestigd, dus het contact was snel gelegd. COMEX kwam met Silent Bricks van Fast LTA. Daarmee gebeurt de replicatie automatisch. De brick kun je uit het systeem nemen en offline bewaren. Dat is essentieel. Afhankelijk van de back-upstrategie verwissel je bijvoorbeeld eens per week de brick en dat scheelt enorm veel werk in vergelijking met tapes bijvoorbeeld. Het is een geruststellend gevoel om te weten dat in de kluis nog een replica ligt van de gehele back-up. Dat gevoel heb ik niet als een back-up direct aan het netwerk is verbonden.”

“Zelfs de meest geavanceerde bedrijven worden gehackt, dan moeten we als gemeente Vaals niet de illusie hebben dat we slim genoeg zijn om hackers buiten te houden.”

Erik Winands – systeem- en netwerkbeheerder, gemeente Vaals

De gemeente Vaals gebruikt met de nieuwe oplossing FAST LTA Silent Bricks als back-up doel voor Veeam en bewaart vervolgens de automatisch door het storage systeem gemaakte replica air-gapped in de kluis. Bijkomend voordeel van deze werkwijze ten opzichte van bijvoorbeeld tape is dat de replica een 100 procent identieke kopie van het disk-to-disk back-up is. Met alle voordelen van dien, zoals onmiddellijke random access, instant recovery en geen lastig heen en weer spoelen van bandjes om bestanden op te zoeken. Het is hetzelfde alsof je het originele back-up nog zou hebben.

Air-gapped back-up

Bij een air-gapped back-up wordt de storage met de kopie back-up offline gehaald en bewaard op een veilige plaats. Omdat deze back-up niet met het netwerk is verbonden, is deze onbereikbaar voor hackers. “Als hackers eenmaal binnen in je netwerk zijn, is het een kwestie van minuten. Op dat moment moet je je infrastructuur en data goed op orde hebben en veilig hebben staan om ongeschonden uit de strijd te komen. Een air-gapped back-up is dan een essentieel onderdeel. Sterker nog: vanuit normering van de VNG wordt een air-gapped back-up bijna verplicht gesteld.

Storageplatforms?

In tegenstelling tot veel andere gemeenten in de omgeving heeft Vaals ervoor gekozen om ICT-kennis binnenboord te houden. Erik: "Ik zie bij collega's dat ICT vaak volledig wordt uitbesteed bij een ICT-dienstverlener. Daarmee is de technische knowhow enigszins verdwenen. Op zich geen probleem, maar deze dienstverleners werken vaak op dezelfde manier. Ze schrijven data weg op een storageplatform, maar maken meestal geen air-gapped back-up, dus een back-up die je letterlijk losmaakt van het netwerk. Maar zo is alles wel digitaal met elkaar verbonden en dus bereikbaar voor hackers. Vreemd genoeg zie ik weinig air-gapped back-upoplossingen."

Uitdagingen

Moderne ransomware-hackers maken tegenwoordig eerst de back-ups met data onbruikbaar, voordat de schadelijke software geactiveerd en de waardevolle data versleuteld worden. Zo ook bij meerdere Nederlandse gemeentes. Reden genoeg voor de Vereniging van Nederlandse Gemeentes om het advies uit te brengen ook een kopie van de back-up buiten het bereik van de hackers te hebben. De gemeente Vaals zocht een betrouwbare oplossing voor deze air-gap functionaliteit die de nadelen van een tape-gebaseerd back-up oplost en ook een snelle restore vanuit dit extra beveiligde back-up biedt. Idealiter moest de oplossing gecertificeerd zijn voor de door de gemeente Vaals gebruikte Veeam back-up software.

Soepele implementatie

De implementatie van de Silent Bricks door COMEX verliep soepel. Omdat het om een overheid gaat, moet het budget voor deze uitgave uiteraard verantwoord worden. "Maar we zagen zoveel heil in deze oplossing, dat COMEX in de periode tot de definitieve goedkeuring een huurunit heeft geplaatst. Zo konden we alvast met de Silent Bricks werken en wennen aan het systeem. De implementatie was daarna heel eenvoudig, ik denk dat COMEX een uur bezig is geweest en het werkt sindsdien als een zonnetje." Voor bedrijven is de uitgave misschien makkelijker te verantwoorden, denkt Erik. "Er moet geld verdiend worden en als het bedrijf stilligt door een cyberaanval, kost het geld. Plus dat allerlei gegevens van klanten op straat komen te liggen. Dat wil je altijd voorkomen."

Oplossing

Silent Brick systeem met
1x Drive G2000 Pro
3x Silent Brick 16/24 TB

Branche

Overheid / Gemeente

Toepassing

Veeam Backup & Replication

