CASE STUDY **BESCHERMING TEGEN RANSOMWARE**

Gemeentes staan onder druk - Cybercriminelen zien de kwetsbaarheid van deze overheidsinstellingen: privacy gevoelige data; veel medewerkers die toegang tot deze data hebben. Dit maakt deze sector tot een gewild slachtoffer. Gemeente Veenendaal werd ook getroffen door een attack en nam daarop concrete maatregelen om zich tegen Ransomware te beschermen.

GEMEENTE VEENENDAAL

EINDGEBRUIKERS BESCHERMEN TEGEN ZERO-DAY AANVALLEN

Gemeente Veenendaal is een jonge leefstad met zo'n 65.000 inwoners. De gemeente profileert zich als ICT-centrum en probeert actief ICT-bedrijven aan te trekken. Veenendaal wil hierin een voortrekkersrol nemen en zeker ook in IT-security. Digitale beveiliging is met de komst van de Baseline Informatiebeveiliging Gemeenten (BIG) en de Meldplicht Datalekken voor iedere gemeente een belangrijk aandachtspunt geworden. De gemeente Veenendaal vertrouwt hiervoor op oplossingen van Trend Micro, dat onlangs door Gartner is uitgeroepen tot end point security leader

ICT staat in Veenendaal centraal en de stad beschikt over uiteenlopende initiatieven op het gebied van ICT. Denk bijvoorbeeld aan een ICT-campus die door Veenendaal is opgezet, waarbij de gemeente nauw samenwerkt met opleidingsinstituten en ICT-bedrijven in Veenendaal. Hier worden opleidingen op het gebied van ICT verzorgd. "Daarnaast beschikt Veenendaal over een 'ICT & Food Valley Kring'. Dit is een netwerkgroep waar ICT-bedrijven, ondernemers en ICT'ers elkaar ontmoeten en ideeën kunnen uitwisselen. Dit leidt tot allerlei interessante samenwerkingen in de regio", zegt Karel Klumpenaar, teamcoördinator ICT en Inkoop bij de gemeente Veenendaal.

Samenwerking met gemeente Rhenen

Ook intern wordt binnen de gemeente Veenendaal uiteraard gebruik gemaakt van ICT. De ITomgeving van de gemeente wordt beheerd door een team van 11 ICT-specialisten. Klumpenaar: "We werken nauw samen met de gemeente Rhenen, waarmee we een twin datacenter concept hebben opgezet. Beide gemeenten werken vanuit hun eigen datacenter en vormen voor elkaar een uitwijklocatie. Indien het datacenter in Veenendaal problemen geeft kunnen onze ambtenaren verder werken vanuit het datacenter in Rhenen."
"We bieden inmiddels een jaar of vijf virtuele desktops aan voor onze gebruikers. Dit geeft hen de mogelijkheid vanaf iedere locatie in dezelfde virtuele omgeving te werken, bijvoorbeeld onderweg of vanuit huis. De virusscanners die wij voorheen gebruikten zorgden echter voor een flinke belasting op de beschikbare capaciteit, wat de gebruikerservaring niet ten goede kwam. We zijn daarom op zoek gegaan naar een concurrerende oplossing die minder capaciteit vereist."

Ransomware

Klumpenaar legt uit: "Daarnaast zagen we ongeveer anderhalf jaar geleden bij allerlei collegagemeenten veel narigheid ontstaan door ransomware, een vorm van kwaadaardige software die data in gijzeling neemt door deze te versleutelen. Ransomware kan de bedrijfsvoering ernstig verstoren, leiden tot financiële schade en in het ergste geval zelfs dataverlies tot gevolg hebben. We zijn daarom op zoek gegaan naar een oplossing waarmee we actief ransomware kunnen opsporen en buiten de deur kunnen houden. Voorkomen is immers altijd beter dan genezen".

"Naast ransomware hebben wij te maken met gerichte aanvallen op onze IT-infrastructuur,
waarbij aanvallers meerdere aanvallen combineren om onze infrastructuur binnen te dringen. Dit worden ook wel Advanced Persistent Threats (APT's) genoemd. Samen met ransomware zorgt dit voor veel extra werk, terwijl wij geen extra mankracht of budget beschikbaar krijgen om dit op te pakken. De grote uitdaging waar wij voor stonden was dan ook meer te doen met dezelfde capaciteit."

Gemeente Veenendaal beschikt over een IT-afdeling van elf man. Dit team verzorgt en beheert 810 virtuele werkplekken voor medewerkers van de gemeente. Daarbij heeft de gemeente in samenwerking met gemeente Rhenen een Twin datacenter opgezet en vormen zo een uitwijklocatie voor elkaar.

Als veel gemeenten had ook Veenendaal te maken met Ransomware en gerichte aanvallen op de IT-infra-structuur. "Trend Micro Deep Discovery neemt het hele netwerk onder de loep en spoort voor ons dreigingen op en pakt deze aan. In het dashboard zien we dat er meerdere bedreigingen zijn tegengehouden, waardoor vermoedelijk schade is voorkomen. Hoeveel schade is helaas niet te meten. Daarnaast merken we dat we met dezelfde mankracht meer werk kunnen verrichten" aldus Karel Klumpenaar, teamcoördinator ICT gemeente Veenendaal.

RESUMÉ

Direct inzicht in uw netwerk door Deep Discovery van Trend Micro. Een oplossing die relatief snel te implementeren is, zonder infrastructurele aanpassingen en performance verlies. Onafhankelijke beoordeling toont bovendien aan dat deze oplossing bovenaan in ranking staat. Dit maakt de keuze voor Trend Micro Deep Discovery tot de best mogelijke.

Trend Micro Enterprise Security Suite

Sinds vier jaar maakt de gemeente Veenendaal gebruik van Trend Micro Enterprise Security Suite (ESS) met OfficeScan. “Deze oplossing scant onze virtuele machines op virussen, malware en andere kwaadaardige software”, zegt Klumpenaar.
“We hebben hierbij bewust voor Trend Micro gekozen door de specifieke ondersteuning die zij met ESS voor virtuele machines bieden. Dankzij de Virtual Desktop Infrastructure (VDI) plugin is ESS in staat virtuele machines veel efficiënter te scannen dan traditionele antivirussoftware. Daarnaast is de software erg gebruiksvriendelijk.”

Interne netwerk scannen op dreigingen

“Om onszelf en onze data te beschermen tegen ransomware zijn we in 2015 op zoek gegaan naar een oplossing die het interne netwerk scant op dreigingen. Veel oplossingen beperken zich tot de rand van het netwerk en proberen hier dreigingen tegenhouden. Weet zo’n dreiging toch het netwerk binnen te komen, dan heeft het hier vaak vrij spel. Trend Micro Deep Discovery neemt het interne netwerk onder de loep en kan hierdoor dreigingen van binnenuit detecteren. Deze oplossing hebben we in het derde kwartaal van 2015 geïmplementeerd”, legt Klumpenaar uit. “Wie al een beveiligingsoplossing van een bepaalde fabrikant gebruikt is al snel geneigd opnieuw voor dezelfde fabrikant te kiezen. Bij de keuze voor Deep Discovery hebben we toch opnieuw een marktanalyse uitgevoerd. Hier kwam Trend Micro echter opnieuw als de beste uit de bus. Deep Discovery kan worden geïntegreerd in ESS. Zo kan Deep Discovery ESS automatisch inlichten over nieuwe dreigingen, zodat ESS hier gericht naar kan zoeken. De keuze voor Trend Micro lag dan
ook voor de hand.”

Gedrag analyseren

Een belangrijk voordeel van Deep Discovery is het feit dat deze oplossing naar gedrag kijkt, en niet zoals veel andere oplossingen naar zogeheten ‘signatures’ van malware, zo vertelt Karel Klumpenaar. “Deze signatures worden aangemaakt door beveiligingsbedrijven, wat alleen mogelijk is voor bekende en eerder gedetecteerde malware. Signatures zijn dus niet beschikbaar voor nieuwe malware, die nog niet eerder is opgedoken. Door naar verdacht gedrag te zoeken kan Deep Discovery ook dreigingen opsporen en aanpakken die andere oplossingen niet kunnen detecteren.”
“De implementatie van beide oplossingen is soepel verlopen. Bij de implementatie van ESS hebben wij ondersteuning gekregen van B-Able. De samenwerking met deze partij is prettig verlopen. Bij de implementatie van Deep Discovery hebben we ondersteuning gekregen van de Trend Micro partner Avensus. Samen hebben we een proof-of-concept ontwikkeld, waardoor we precies wisten wat we konden verwachten. De uiteindelijk uitrol van de oplossing was hierdoor relatief eenvoudig en kon vrij snel worden uitgevoerd.”

Meerdere dreigingen tegengehouden

De gemeente Veenendaal is erg tevreden over zowel ESS als Deep Discovery. In het dashboard zien we dat beide oplossingen meerdere dreigingen hebben tegengehouden, waardoor vermoedelijk schade is voorkomen. “Hoeveel schade hiermee precies is voorkomen is helaas niet te meten”, aldus Klumpenaar. “Daarnaast merken we dat we met hetzelfde budget en dezelfde hoeveelheid mankracht meer werk kunnen verrichten, doordat we met de oplossingen taken kunnen automatiseren. Zo worden zowel interne als externe dreigingen in veel gevallen geautomatiseerd tegengehouden. Dit scheelt ons veel tijd.”
Tot slot vertelt Klumpenaar: “We kijken op dit moment naar mogelijkheden om onze Fortigate firewall te integreren met Deep Discovery. Indien een dreiging wordt gedetecteerd, willen we dat Deep Discovery hierover automatisch de firewall inlicht. Indien nodig kunnen poorten worden afgesloten, IP-adressen geblokkeerd of andere maatregelen worden genomen. Dergelijke automatisering neemt ons veel werk uit handen en is dan ook erg welkom.”