ICT CENTRAAL IN NEDERLAND

‘WE BRENGEN ANALYSETIJD TERUG VAN DAGEN NAAR SECONDEN’

Mark Beunk,
channel manager Benelux and Nordics bij Carbon Black

Met de komst van Carbon Black kent de Nederlandse markt nu drie jaar een leverancier van proactieve security. Hoewel anderen dat ook claimen, gaat de Amerikaanse securityspecialist naar eigen zeggen verder door meerdere lagen in endpoint security.

door: Michiel van Blommestein

Nog niet zo lang geleden werkte security vrijwel geheel volgens het principe van handtekeningen. Als nieuwe malware verschijnt, stoppen de security-leveranciers de kenmerken in een database zodat anti-malware deze kan herkennen. Toen kon dat ook nog, zegt Channel Manager Benelux and Nordics Mark Beunk van Carbon Black. “Twintig jaar geleden kwamen er 1.000 nieuwe stukken malware uit en dan kun je in een database prima bijhouden. Maar nu komen er duizend per seconde bij en dan win je de oorlog niet met een signature based aanpak.”

Misbuik van processen

Ondertussen gaat 53 procent van de aanvallen niet met klassieke malware, zegt Beunk. “Het is niet meer een bestandje op de harde schijf maar het gaat om misbruik van bestaande, goedgekeurde processen. Iemand op kantoor laat zijn collega’s een filmpje zien op een geïnfecteerde website en via de flash player wordt een powershell gestart waarmee code wordt geïnjecteerd. Omdat er niets op de harde schijf terecht komt, is er volgens de antimalware geen breach.” Security heeft de laatste jaren belangrijke ontwikkelingen doorgemaakt. Het probleem is volgens Beunk dat de meeste oplossingen op zichzelf hun eigen nadelen hebben. “Veel nieuwe partijen passen bijvoorbeeld machine learning toe. Als iets ovaal is en groen, dan zal het wel een druif zijn. Probleem is dat het ook een olijf kan zijn. Je krijgt dan dus een false positive of false negative.”

Gelaagd

Daarom gaat Carbon Black verder op het gebied van endpoint security. “We hebben een gelaagde aanpak met sandboxing, handtekeningen, machine learning en streaming prevention in één agent”, legt Beunk uit. “Zo kunnen we de gemiddelde analysetijd die specialisten nodig hebben, terugbrengen van dagen naar seconden. Belangrijk want snelheid stopt breaches, zeggen wij.” Streaming prevention, de meest opvallende van de vier gebruikte technieken, is volgens Beunk een soort camera die alles opneemt wat op een endpoint plaatsvindt. “Zo kunnen we een risicoprofiel creëren.” Dat werkt ook goed op apparaten met één duidelijke functie die op onder meer een verouderd besturingssysteem draaien. “Als je een pinautomaat hebt, dan weet je dat die maar één doel heeft: pas erin, pincode intoetsen en geld uitgeven. De rest kun je dus blokkeren.”

Carbon Black is dus een specialist die op zijn specialisatie heel breed kijkt. “Breed is relatief”, zegt Beunk. “We werken via open API’s samen met technologiepartners om ook andere gebieden te beveiligen. Denk aan SIEM of netwerkbeveiliging.” Carbon Black is pas drie jaar actief in Nederland, maar bestaat in de VS al 14 jaar. Ervaring en referenties genoeg dus, zegt Beunk. “We hebben Wannacry weten te voorkomen bij een grote klant met 120.000 endpoints.” «

www. carbonblack.com mbeunk@carbonblack.com 06 411 06 254 @CarbonBlack_Inc