Intrusion Detection Systems blijven onmisbaar

Stevige afweer houdt meeste problemen buiten de deur

Dertien jaar geleden verklaarde Gartner Intrusion Detection Systems (IDS) dood. Twee jaar had IDS nog, dacht het onderzoeksbureau toen. Gartner had de plank niet meer mis kunnen slaan. De rol van IDS is sindsdien gegroeid en de systemen maken zelfs de overstap naar de cloud.

door: TANJA DE VREDE / T.D.VREDE@AUTOMATISERINGGIDS.NL
beeld: DE BEELDREDAKTIE / GUIDO BENSCHOP

De kritiek van Forrester op Intrusion Detection Systems (IDS) was niet mals dertien jaar terug. Het kostte organisaties te veel tijd en moeite om full time te monitoren, stelde het onderzoeksbureau vast. IDS leverde voornamelijk false positives op, waardoor beheerders terechte waarschuwingen niet meer serieus namen. Bovendien registreerden en meldden de IDS'en alleen maar, blokkeren deden ze niet. Ook was IDS erg arbeidsintensief om te beheren, want veel moest met de hand. Oh ja, het leverde enorme bergen data op waar toentertijd bijna niets mee te doen was voor beveiligers, juist door die omvang.

Toch is IDS niet verdwenen, zoals Gartner voorspelde. Veel van de technieken van IDS zijn ondergebracht in Intrusion Prevention Systems, die daarom vaak Intrusion Detection and Prevention Systems worden genoemd. Immers, alleen detectie volstaat niet voor een adequate beveiliging, maar goede detectie is wel weer van cruciaal belang voor preventie en voor respons.

Netwerk en host based

De twee belangrijkste typen IDS zijn het netwerkgebaseerde en het host based IDS. Het netwerkgebaseerde IDS monitort netwerkverkeer op verdachte en afwijkende activiteiten. Ze worden op strategische punten in het systeem geplaatst en kijken naar de packets die binnen het netwerk verstuurd worden. Met deze data kan het IDS aanvallen, verdacht verkeer en gedrag dat afwijkt van de regels herkennen en dit verkeer als zodanig aanmerken. Het blokkeert geen netwerkverkeer – de rol van het systeem is passief – er wordt alleen verzameld, geïdentificeerd, gelogd en gealarmeerd.

Een bekend en veel gebruikt netwerkgebaseerd IDS is SNORT.

»

SNORT is een open source IDS dat real time verkeer analyseert en packets logt op IP-netwerken. Daarbij biedt het analyses van de protocollen en zoekt en vergelijkt het content. SNORT detecteert aanvallen of wat daarop lijkt, zoals buffer overflow en port scans. Het is inmiddels voorzien van functionaliteit om ook zelf te reageren op de gevonden bedreigingen en valt daarom onder de noemer IDPS.
Een host based IDS monitort verdachte en afwijkende activiteiten op specifieke apparaten binnen het netwerk. Dat gebeurt met behulp van agents; elk apparaat wordt voorzien van een agent die in- en uitgaande packets van het apparaat monitort. Een veelgebruikte methode hierbij is dat de agent snapshots neemt van bestaande systeembestanden en die vergelijkt met eerdere snapshots. Zijn de kritieke systeembestanden gewijzigd of verdwenen, dan slaat de host based IDS alarm. De agent werkt met een combinatie van signatures, regels en heuristiek om die activiteiten te herkennen.

Drie uitdagingen

Eelco Stofbergen, thought leader cybersecurity en director consulting services bij IT-dienstverlener CGI, ziet dat detectie steeds belangrijker wordt. “Het detecteren van incidenten komt op, maar wordt nog onvoldoende gebruikt. In het algemeen hebben monitoring en detectie voor security nog stappen te maken.”
Hij begrijpt waarom detectie nog niet overal gebruikt wordt. “Het is een complex onderwerp dat diverse kwaliteiten vraagt, kwaliteiten waarover veel organisaties niet beschikken”, zegt Stofbergen. “Effectief gebruik van intrusion detection in organisaties kent drie grote uitdagingen. Allereerst vereist het configureren van apparaten en het inrichten in het netwerk veel kennis. Grotere organisaties kunnen dat vaak wel, die hebben de expertise daarvoor in huis. Kleinere organisaties hebben die kennis meestal niet. Vaak ook worden verkeerde detectieregels ingevoerd waardoor er te veel false positives optreden en het detectieproces onwerkbaar wordt.”
Ten tweede moet de organisatie in staat zijn adequaat te reageren als een incident wordt gedetecteerd en dat lukt velen niet. Uit een recent onderzoek van IT-dienstverlener CGI onder duizend beslissers bleek dat een op de drie bedrijven geen goed reponsplan heeft. Zo’n plan komt vaak pas nadat men een ernstig incident heeft meegemaakt. En herkennen ze een probleem wel als er een melding van komt?
Als laatste moet een IDS gevoed worden met informatie. Ook dat is niet eenvoudig. Stofbergen: “Het systeem moet van de juiste informatie worden voorzien, dus met de juiste regels als het rule based is. Ook een IDS dat met ‘threath intelligence’ werkt is in opkomst: actuele informatie over dreigingen, indicatoren die beschrijven waaraan een aanval te herkennen is [zie kader]. Daarmee kan het detectiesysteem dan de nieuwste aanvallen detecteren.” Bepaalde karakteristieken in de code kunnen op malware duiden, zegt Stofbergen. “Het systeem moet op actuele dreigingen inspelen, want criminelen omzeilen de detectie die zich op oudere informatie baseert. Aanvallen worden ontworpen met nieuwe software, nieuwe malware, andere IP-adressen waarmee verbonden wordt.”

IDPS-as-a-Service

De drie punten oppakken lukt veel bedrijven niet. Organisaties nemen hiervoor gespecialiseerde partijen in de arm die IDS als een dienst aanbieden. “Alleen al 24/7 monitoren is ingewikkeld om te regelen, want je hebt voor elke functie minimaal drie mensen nodig”, zegt Stofbergen.
Onderzoek van Forrester uit 2015 onder ruim 3500 beslissers wereldwijd geeft aan dat 31 procent ook van plan is IDPS-as-a-Service aan te schaffen. Een tekort aan deskundig personeel is daarvoor de belangrijkste reden.
Ook de kosten die IDS met zich meebrengt, maakt veel organisaties terughoudend. Stofbergen: “IDS kan duur zijn, maar aan de andere kant wordt de impact van incidenten steeds groter. Daardoor is goede monitoring vaak toch de investering waard. Daarnaast wordt monitoring en detectie door steeds meer toezichthouders verplicht gesteld.”
De kosten van IDS kunnen wel lager worden gehouden door het zelf te doen en dan voor een opensource-oplossing te kiezen. Voor kennis kan men – deels – terecht bij community’s. “Goede detectie blijft specialistisch werk. Je kunt voor een externe leverancier kiezen, maar niet alles permanent laten monitoren. Dan is het belangrijk dat je een beter inzicht hebt in wat je kritieke assets zijn en daar je monitoring op te richten.” Helaas heeft een groot deel van de organisaties dat juist niet op orde.

EELCO STOFBERGEN, CGI:
‘DE IMPACT VAN INCIDENTEN WORDT STEEDS GROTER. DAARDOOR IS GOEDE MONITORING VAAK TOCH DE INVESTERING WAARD.’