Intrusion detection als probaat middel tegen inbraak

Marcel Spruit

Intrusion detection, het detecteren van elektronische indringers, kan een waardevolle aanvulling zijn op de beveiligingsmaatregelen voor het bedrijfsnetwerk. Het inzetten van een intrusion detection systeem (IDS) heeft echter nogal wat voeten in de aarde. Dit artikel gaat in op wat een IDS is, en wat er zoal komt kijken bij het inzetten ervan.

Vrijwel elk bedrijf heeft tegenwoordig een intern netwerk, waarop verscheidene servers en een grote hoeveelheid pc's en randapparatuur aangesloten zijn. Veel van die netwerken zijn ook nog verbonden met het Internet. Dat biedt legio mogelijkheden, zoals het versturen van elektronische post, het communiceren met klanten en leveranciers, het transporteren van software, en nog veel meer. Bovendien kan een Internetverbinding gebruikt worden om bijvoorbeeld thuiswerkers toegang te geven tot gegevensbestanden die anders alleen via het interne netwerk te benaderen zouden zijn.
Naast de vele voordelen heeft het maken van een verbinding tussen een intern netwerk en het Internet echter het nadeel dat de wereldwijde gemeenschap van hackers ook gebruik kan maken van dezelfde verbinding. Elk zichzelf respecterend bedrijf dat aangesloten is op het Internet, heeft dan ook een firewall om al het gegevensverkeer tussen het interne netwerk en het Internet te controleren en ongewenste bezoekers buiten te houden [Zwicky, Cooper & Chapman].

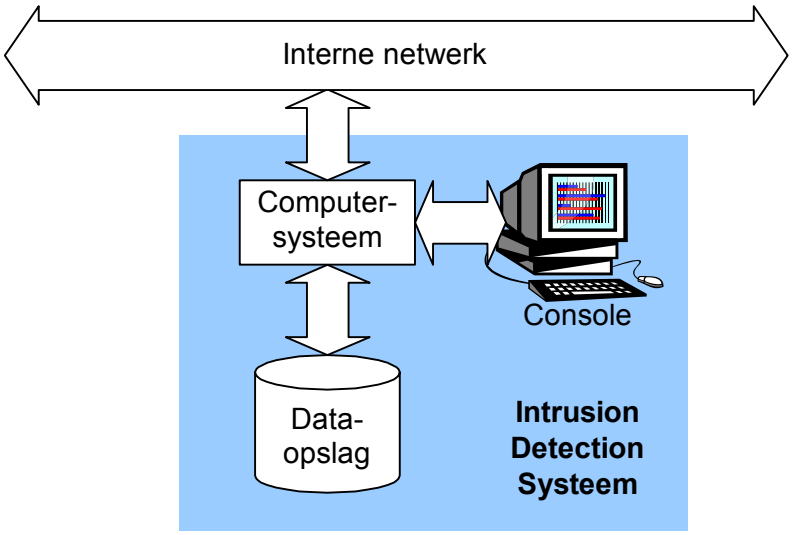
Echter, hoe nuttig een firewall ook is, de beschermende werking ervan is beperkt. De belangrijkste beperking van een firewall is dat deze het langskomende gegevensverkeer slechts in beperkte mate kan controleren. Een firewall fungeert als een sluis tussen het interne netwerk en het Internet, zodat al het ingaande en uitgaande verkeer langs de firewall komt. Als een waterdichte controle hiervan al mogelijk zou zijn, dan zou het veel te veel tijd vergen. Om de verkeerscapaciteit niet al te ongunstig te beïnvloeden, controleert een firewall daarom slechts een beperkt aantal aspecten van het langskomende verkeer. Hierdoor ontstaat echter wel een zwakke plek in de beveiliging die door een hacker misbruikt kan worden om op het interne netwerk in te breken.
Een andere belangrijke beperking van de firewall wordt niet zozeer bepaald door de firewall zelf, maar door de plaats ervan. Een firewall kan namelijk alleen beschermen tegen ongewenst verkeer van buiten (het Internet). De eigen medewerkers, die direct toegang hebben tot het interne netwerk, hoeven voor hun activiteiten helemaal niet door de firewall. Uit vele onderzoeken blijkt dat juist de eigen medewerkers veelal voor de grootste problemen zorgen [Spruit & Looijen]. Weliswaar is het leeuwendeel van de intern veroorzaakte problemen gestoeld op fouten en vergissingen, die dus te goeder trouw gemaakt worden, maar ze leiden desondanks toch tot verstoringen.

In een bedrijfssituatie is er behoefte aan maatregelen die de beschermende werking van een firewall aanvullen. Het intrusion detection systeem (IDS) is zo'n maatregel. Als de firewall beschouwd wordt als de portier bij de voordeur die iedereen controleert die

het gebouw in of uit wil, en zonodig ongewenste individuen tegenhoudt, dan kan het IDS beschouwd worden als het inbraakalarm dat afgaat op het moment dat in het gebouw een indringer gesignaleerd wordt. Bovendien kan het IDS ook ongewenste activiteiten van eigen medewerkers op het interne netwerk detecteren.

Wat is een IDS

Een intrusion detection systeem (IDS) is een systeem dat verdacht netwerkverkeer op het interne netwerk detecteert. Het kan daarbij gaan om verkeer dat niet door de firewall tegengehouden is, of verkeer dat de firewall nooit gepasseerd is. Een IDS wordt daarvoor aangesloten op het interne netwerk, waarna het continu het netwerkverkeer afluistert en analyseert (zie Figuur 1).



Figuur 1: Een netwerk met een IDS

Als een IDS direct na een verdachte activiteit alarm moet kunnen slaan, dan is het nodig dat al het langskomende gegevensverkeer na het aftappen direct (realtime) geanalyseerd wordt. Hiervoor is een voldoende grote verwerkingscapaciteit nodig, waarvoor bij een gemiddeld netwerk al gauw kostbare apparatuur en programmatuur nodig zijn. Het is echter ook mogelijk dat een IDS alleen wordt gebruikt om in voorkomende situaties te kunnen achterhalen of er daadwerkelijk ongewenste activiteiten plaatsgevonden hebben. In dat geval wordt het afgetapte netwerkverkeer voorbewerkt en vastgelegd, maar de analyse ervan vindt alleen plaats (off-line), nadat er een verdenking gerezen is.

Als een realtime werkend IDS in het netwerkverkeer een verdachte activiteit ontdekt, dan slaat het alarm. Dit kan zowel een stil alarm zijn, als het waarschuwen en gelijktijdig blokkeren van de verdachte activiteit. In het eerst geval krijgen de gealarmeerde beheerders de mogelijkheid om de verdachte activiteit te bestuderen. Dit kan belangrijk zijn voor het vergaren van bewijsmateriaal dat nodig is voor het vervolgen van een ongewenste bezoeker. Het waarschuwen en meteen dichtgooien van de ‘deur’ is welis-

waar veiliger, omdat de ongewenste activiteiten gestopt worden, maar heeft het nadeel dat de indringer zich veilig terug kan trekken. Bovendien wordt in het geval van een vals alarm een normale gebruiker in zijn werk gehinderd.

Om voldoende informatie te vergaren over eventuele indringers, wordt ook wel gebruik gemaakt van zogenaamde honeynets. Een honeynet bestaat uit één of meer computersystemen die niet gebruikt worden voor normale bedrijfsactiviteiten, maar die alleen bedoeld zijn om indringers aan te trekken en te bestuderen. Voor indringers van buiten lijken zulke systemen precies op gewone bedrijfssystemen. Als een indringer in een honeynet zit, dan kunnen de beheerders ervan op hun gemak de activiteiten van de indringer bestuderen en vastleggen, zonder dat het negatieve gevolgen heeft voor de normale bedrijfssystemen.

Soorten IDS

Er kunnen twee soorten IDS'en onderscheiden worden, namelijk [Kanters]:
- host-based IDS;
- network-based IDS.

Een host-based IDS werkt met intrusion detection software die geïnstalleerd wordt op een te beschermen computersysteem. Het voordeel daarvan is dat het IDS zeer gericht het doelsysteem beveiligt. Bovendien werkt het ook tegen verdachte activiteiten die niet via het netwerk gaan, maar bijvoorbeeld via het toetsenbord of een CD. Het nadeel is echter dat het IDS een zware belasting vormt voor het te beveiligen systeem. Bovendien komt een eventuele indringer zo wel erg dicht bij de waardevolle gegevens, en ook bij het IDS zelf. Het is zelfs mogelijk dat de indringer het IDS onklaar kan maken, voordat het in actie komt.

Een network-based IDS bestaat uit een speciaal daarvoor bestemd computersysteem met bijbehorende software. Het IDS wordt aangesloten op het netwerk dat beveiligd moet worden, waarna het vervolgens al het langskomende netwerkverkeer aftapt. Een network-based IDS vergt dus een eigen computersysteem, dat bovendien voldoende capaciteit moet hebben om al het langskomende gegevensverkeer af te tappen. Met het IDS kunnen dan wel meerdere computersystemen tegelijk bewaakt worden.

Om te bepalen of er iets verdachts gebeurt, maakt een IDS gebruik van een verzameling bekende aanvalspatronen. Als een nieuwe aanval gedetecteerd is, dan wordt naar een karakteristiek patroon gezocht, een 'handtekening'. Deze handtekening wordt toegevoegd aan de verzameling van eerder bepaalde handtekeningen. Het duurt echter een tijdje voordat een nieuw ontwikkelde aanval is gedetecteerd en gekarakteriseerd. En als een aanval gekarakteriseerd is, dan moet de handtekening nog aan de verzameling in een IDS toegevoegd worden. Pas dan kan de aanval door het betreffende IDS gedetecteerd worden. De beheerder van een IDS zal er daarom steeds voor moe-

ten zorgen dat de handtekeningenverzameling van zijn IDS up-to-date gehouden wordt.[1]

Een andere aanpak om verdacht netwerkverkeer op te sporen is gebaseerd op statistische analyse van het netwerkverkeer [Marchette]. Daarbij wordt verondersteld dat een IDS kan bepalen welk netwerkverkeer normaal is. Als er dan afwijkingen gedetecteerd worden ten opzichte van het normale gedrag, dan wijst dat op verdachte activiteiten. Het IDS moet dan eerst 'leren' welk netwerkverkeer als normaal beschouwd kan worden. Hiervoor meet het systeem gedurende langere tijd aan het netwerkverkeer, waarna allerlei grenswaarden bepaald en ingesteld worden. Een belangrijk nadeel van een dergelijke aanpak is de grote kans op vals alarm, doordat elke uitzondering in principe tot verdacht bestempeld wordt, terwijl het vaak het resultaat is van een onschuldige fout of experimenteergedrag van een medewerker. Bovendien moeten de grenswaarden elke keer dat de gebruikersomgeving verandert opnieuw bepaald en ingesteld worden.

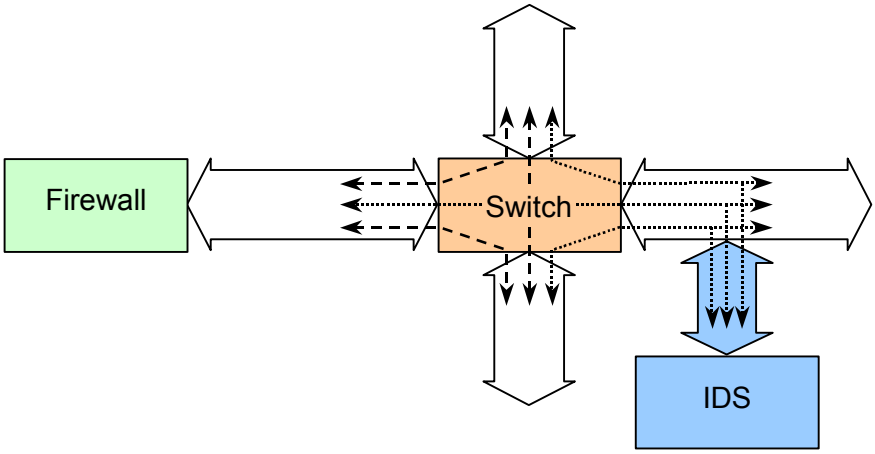
IDS'en zijn als commerciële producten verkrijgbaar, maar ook als freeware en shareware producten [Cerias]. Er zijn zelfs open-source IDS-oplossingen beschikbaar [Snort]. Open-source en andere freeware producten zijn weliswaar goedkoop te verkrijgen, maar daar staan wel meer beheerinspanningen tegenover. Commerciële oplossingen zijn niet goedkoop, maar er komt dan wel een product met bijbehorende service binnen.

De plaats van een IDS

Een host-based IDS wordt geïnstalleerd op een te bewaken computersysteem. Een network-based IDS kan daarentegen op verschillende plaatsen opgesteld worden. Als een network-based IDS achter de firewall (aan de 'binnenkant') aan het interne netwerk gekoppeld is, dan werkt het als een inbraakalarm, waarmee indringers en ongewenste activiteiten van medewerkers gedetecteerd worden. Als er behoefte is om inbraakpogingen al te detecteren voordat ze succesvol zijn, dan moet het IDS vóór de firewall (aan de 'buitenkant') geplaatst worden. In dat geval is het IDS wel kwetsbaarder voor aanvallen die direct op het IDS zelf gericht zijn.

Als een IDS aan het interne netwerk gekoppeld is om het netwerkverkeer te controleren, dan moet al het te controleren verkeer wel langs het IDS komen. Een netwerk van enige omvang bevat echter al gauw een stuk of wat netwerkcomponenten die het netwerkverkeer reguleren [Ek]. Zo zijn er bijvoorbeeld routers waarmee het netwerk gesegmenteerd wordt, en switches waarmee het verkeer direct naar de juiste bestemming geloodst wordt. In dat geval komt er alleen nog maar 'bestemmingsverkeer' langs het IDS (zie Figuur 2).

[1] Er is een duidelijke analogie te zien met de 'handtekeningen' van virussen waarmee antivirussoftware werkt.



Figuur 2: Een IDS achter een switch ziet alleen 'bestemmingsverkeer'

Sommige switches zijn voorzien van een aftappoort, een span-poort, waarnaar al het netwerkverkeer dat de switch passeert kan worden gekopieerd. Als een IDS aangesloten wordt op de span-poort, dan kan deze wel al het netwerkverkeer te zien krijgen dat de betreffende switch passeert. Een nadeel is dat de switch dan extra belast wordt, zodat de capaciteit ervan terugloopt. Overigens kan via een span-poort geen verkeer zichtbaar gemaakt worden dat al door een andere switch weggeloodst is. Als er meerdere switches in het netwerk aanwezig zijn, dan kunnen ze wel ieder apart afgetapt worden. Voor het aftappen van andere netwerksegmenten zijn nog weer meer IDS'en nodig. Hoe meer IDS'en er ingezet worden, hoe hoger de complexiteit en de kosten.

Als een omvangrijk netwerk bewaakt moet worden, dan zal het al gauw nodig zijn om verscheidene IDS'en in te zetten. Eventueel kunnen de IDS'en uitgerust worden met elementaire analysemogelijkheden, waarmee alleen een voorbewerking wordt uitgevoerd. De resultaten daarvan kunnen dan naar een centraal systeem gestuurd worden, waarmee een grondigere analyse uitgevoerd wordt.

Het beheer van een IDS

In de praktijk komt er nogal wat kijken bij het inzetten van een IDS. Het ontwikkelen van IDS'en is zodanig complex, dat dat het beste door gespecialiseerde bedrijven gedaan kan worden. Bovendien kunnen deze bedrijven zich dan ook richten op het inventariseren en karakteriseren van nieuwe aanvalspatronen, om zo de benodigde handtekeningenverzamelingen voor de IDS'en samen te stellen. Voor de meeste organisaties volstaat zo'n standaard IDS. Een standaard IDS moet dan nog wel op de juiste plaats geïnstalleerd worden. Vervolgens moet de IDS zo ingesteld worden dat onderscheid gemaakt wordt tussen normaal en ongewenst verkeer. De hiervoor benodigde grenswaarden zijn echter niet eenvoudig te bepalen. Veelal kost het een zekere leertijd voordat de juiste waarden gevonden zijn.

Overigens moet een IDS zelf bijzonder goed beveiligd worden, want als 'alarminstallatie' is het zelf veelal één van de eerste doelwitten van een indringer. Voor een network-

based IDS gelden dan ook soortgelijke maatregelen als voor een firewall. Dit betekent dat de toegang tot het IDS voorbehouden is aan de beheerders van het systeem. Dit betreft niet alleen de logische toegang, maar ook de fysieke toegang tot de ruimte waarin het systeem staat. Bovendien hoort er op de IDS-computer alleen software te draaien die voor de IDS noodzakelijk is. Om de kans op beveiligingslekken nog verder te verkleinen dienen alle op het systeem beschikbare diensten en protocollen, die niet noodzakelijk zijn voor de IDS-functionaliteit, uitgezet te zijn.

De handtekeningenverzameling die een IDS nodig heeft, veroudert, net als bij een virusscanner, doordat er steeds nieuwe aanvallen bedacht worden. De verzameling moet dan ook regelmatig ververst worden. Nu hoeft dat nog niet zo heel vaak, maar in de naaste toekomst zal deze frequentie naar verwachting snel stijgen. Een zelfde ontwikkeling is te zien geweest bij virusscanners: een goede virusscanner moest nog niet zo heel lang geleden gemiddeld eens per maand geactualiseerd worden, terwijl op dit moment dagelijkse update de norm is. De beheerder van een IDS zal er nu al voor moeten zorgen dat de handtekeningenverzameling regelmatig geactualiseerd wordt. Daarnaast komen er in de loop van de tijd zwakheden in de software van het IDS aan het licht. De leverancier van het IDS zal normaal gesproken reageren met het beschikbaar stellen van patches (reparatieprogrammatuur). De beschikbare patches moeten zo spoedig mogelijk geïnstalleerd worden, omdat de te repareren zwakheden bij derden bekend zijn en dus ook misbruikt kunnen worden.

Een IDS in actie brengt een aanzienlijke hoeveelheid logging voort. Niet alles wat gelogd wordt zal ook tot een alarm leiden. Daarom moeten de beheerders de logging regelmatig analyseren om te controleren of er geen andere sporen van ongewenste activiteiten te vinden zijn. Tevens moeten ze bedacht zijn op incidentele en structurele veranderingen in het gebruik van het netwerk. Als het gebruik structureel verandert, dan heeft dat consequenties voor de ingestelde grenswaarden. Zowel het analyseren van de logging als het opnieuw instellen van grenswaarden zijn in het algemeen zeer tijdrovende bezigheden.

Als een IDS een alarm geeft, dan moet de beheerder de gelogde gegevens analyseren. Tevens moeten er activiteiten ondernomen worden om verdere schade te voorkomen, zoals bijvoorbeeld het blokkeren van een verdacht netwerkadres. Als uit de analyse van de gelogde gegevens blijkt dat het geen vals alarm betreft, dan is er sprake van een incident. In dat geval heeft de beheerder veelal meer gegevens nodig. Naast de gegevens die door het IDS gelogd zijn, kan het dan gaan over gegevens die door andere systemen gelogd zijn en gegevens die handmatig bijeengesprokkeld moeten worden. Bovendien moet de beheerder de partij(en) waarschuwen die van dit soort incidenten op de hoogte gesteld moeten worden, waaronder het eigen management en eventueel opsporingsinstanties.

Al met al omvat het beheer van een IDS een flink aantal activiteiten:
- het installeren en instellen van het IDS;
- het beveiligen van het IDS zelf;
- het actueel houden van de handtekeningenverzameling;

- het ‘patchen’ van het IDS;
- het analyseren van de gelogde gegevens;
- het opnieuw instellen van het IDS als het gebruik van het netwerk verandert;
- het documenteren van verdachte activiteiten;
- het melden van incidenten aan de geëigende partij(en).

Verscheidene van deze activiteiten kosten een aanzienlijke inspanning en vergen bovendien bijzondere deskundigheid. Voor veel organisaties is uitbesteding hiervan dan ook een zeer reële optie. Met name als tegelijkertijd ook (een deel van) het beheer van andere beveiligingmiddelen uitbesteed kan worden (bijvoorbeeld de firewall).

Overigens is het inzetten van een IDS alleen zinvol als de beveiliging in z’n geheel goed georganiseerd is. Dit betekent onder meer dat er een beveiligingsbeleid is, dat taken en verantwoordelijkheden voor beveiliging zijn toegewezen, dat de risico’s zijn geanalyseerd, etc. [Overbeek, Roos Lindgreen & Spruit].
Bovendien dienen de meer elementaire beveiligingsmaatregelen al geïmplementeerd te zijn. Hierbij valt te denken aan:
- fysieke maatregelen, zoals bijvoorbeeld brand- en inbraakbeveiliging en noodstroomvoorziening;
- logische maatregelen, zoals bijvoorbeeld log-in/wachtwoordauthenticatie, firewall en antivirus;
- organisatorische maatregelen, zoals bijvoorbeeld functiescheiding, interne controle en incidentenregistratie.

Tenslotte

Het inzetten van een IDS in een bedrijfsnetwerk heeft naast de technische moeilijkheden ook juridische implicaties. Een IDS tapt namelijk niet alleen datacommunicatie van indringers af, maar ook van de eigen medewerkers. Veelal zijn de afgetapte gegevens herleidbaar tot individuele medewerkers. De medewerkers hebben echter bepaalde rechten in het kader van privacybescherming. Dit betekent dat de organisatie haar medewerkers duidelijk moet maken wat wel en niet is toegestaan, en welke datacommunicatie op overtredingen geanalyseerd wordt. Bovendien moeten er regels opgesteld worden over welke gegevens er opgeslagen worden en wie daar toegang toe heeft.

Het inzetten van een honeynet, als aanvulling op een IDS, heeft ook juridische implicaties. Als een hacker bijvoorbeeld een honeynet-computer gebruikt als uitvalsbasis voor hacking-activiteiten elders, dan kan de organisatie die het honeynet beheert daarvoor mede aansprakelijk gesteld worden. Een honeynet kan dan ook niet vrijblijvend geïmplementeerd worden. De beheerders ervan moeten de activiteiten van indringers nauwlettend volgen en tijdig ingrijpen als er risico’s voor derden dreigen. Dit vergt nogal wat inspanning van de beheerders, boven op de aanzienlijke inspanning die het kost om een honeynet goed in te richten.

Ondanks alle haken en ogen kan een IDS, zonodig aangevuld met een honeynet, een belangrijke bijdrage leveren aan het verbeteren van het beveiligingsniveau van een bedrijfsnetwerk. Een IDS vult de beschermende werking van een firewall aan, en kan tevens in de gaten houden of de eigen medewerkers ongewenste activiteiten op het netwerk uitvoeren. Het inrichten en beheren van een IDS is echter een complexe en tijdrovende bezigheid, waarvoor voldoende gekwalificeerde medewerkers nodig zijn. Zonodig kan hierbij gebruik gemaakt worden van uitbesteding aan gespecialiseerde organisaties.

Literatuur

Cerias, http://www.cerias.purdue.edu/coast/ids/ (2002)

P. van Ek, 'Terug naar eenvoud in IP-netwerken', *Telecommagazine*, nr. 8, pag. 32-34 (2002)

F. Kanters, 'Intrusion Detection Systems', *Informatiebeveiliging Praktijkjournaal*, nr. 3, pag. 11-14, 20 (2000)

D.J. Marchette, *Computer intrusion detection and network monitoring: a statistical viewpoint*, Springer, New York (2001)

P. Overbeek, E. Roos Lindgreen & M. Spruit, *Informatiebeveiliging onder controle*, Pearson, Amsterdam (2000)

Snort, http://www.snort.org/ (2002)

M. Spruit & M. Looijen, 'Beveiliging van informatievoorziening', *Informatie*, nr. 5, pag. 328-336 (1995)

E.D. Zwicky, S. Cooper & D.B. Chapman, *Building Internet Firewalls*, O'Reilly, Beijing (2000)