

Innbruddsdeteksjon

Dette er tredje og siste artikkel i en miniserie om *Intrusion Detection* som startet i Mellvik-Rapporten nr. 93.

I de to foregående artiklene har vi diskutert behovene for og utfordringene knyttet til IDS-systemer. Videre har vi gjennomgått en samling overordnede krav det er rimelig å stille til slike verktøy, og presentert teknologiske løsningsvarianter. Turen er kommet til produkter: Evaluering, kriterier, prioriteringer, valg og implementasjon

Dessuten – og minst like interessant: Hvor går veien videre? IDS-systemer – sammen med antivirus og mange andre sikkerhetstiltak vi omgir oss med i det daglige: De er alle reaktive og kurerer symptomer i stedet for den egentlige sykdommen. Er dette en permanent situasjon?

Produkter og krav

Uansett hva fremtiden måtte bringe, har vi konkludert med at IDS-systemer ikke er luksus, men en nødvendighet. Vi har også lagt det faglige grunnlaget for valg av produkter. Neste trinn er å formalisere kunnskapen og utarbeide krav som harmonerer med organisasjonens behov og muligheter: Hva trenger vi – av kompetanse, utstyr og tjenester, hvor mye skal vi gjøre selv, hvilke ressurser har vi til rådighet og så videre. Nest etter erkjennelsen av at IDS-systemer er nødvendige, er klarleggingen av hvem som skal gjøre hva viktigst: Mangler vi kompetanse eller menneskelige ressurser, kan det være aktuelt å sette bort utfordringen til spesialister, og leie tjenester tilbake. Riktignok er tilbudet av slike tjenester mangelfullt på våre breddegrader, men en håndfull leverandører av betydelig størrelse er på plass i USA (se tabellen nedenfor) og andre land, og det rører seg på det hjemlige markedet.

Kriterier

Vårt hovedkriterium er naturligvis produktets evne til å avsløre inntrengninger. Som vi har vært inne på i tidligere artikler, er det imidlertid allerede her en rekke varianter å ta hensyn til: Metodikk, spennvidde, plassering i forhold til objektene som skal sikres og så videre.

Sekundære, men ikke desto mindre viktige kriterier er:

- ✓ Falske alarmer – evnen til å skille støy og regulær trafikk fra de uønskede innslagene.
- ✓ 'Falske negativer' – inntrengninger som ikke blir oppdaget.
- ✓ Ytelse – hvordan trafikken påvirkes.

Andre forhold av stor betydning for produktvalget er:

- ✓ Skalerbarhet – hvor mange systemer trenger vi i dag, og hvilken vekst ser vi for oss de nærmeste årene?
- ✓ Hvordan passer styringsmekanismene inn i etablerte styringsstrukturer?
- ✓ Hvem skal supportere løsningen, hvordan og hvilken løsning gir det beste totale kostnadsbildet?

- ✓ Alle IDS-løsninger – i likhet med virus-scannere – er avhengige av såkalte signaturer for å vite hva de skal se etter. Kontinuerlig oppdatering av signatur-samlingen er en forutsetning for at de skal virke som foreskrevet. Finnes ressursene som trengs for å vedlikeholde denne signatursamlingen? Hvor automatisk og pålitelig kan vedlikeholdet gjøres? Hvilke kilder kan slike signaturer hentes fra? Er vi helt avhengige av leverandøren, eller finnes flere kilder (flere kilder er bedre, og indikerer at formatet er standardisert, en fordel i seg selv)?
- ✓ Er sikkerhetsmekanismene gode nok – for administrasjon, konfigurasjon, logging, oppdatering av signaturer etc.?
- ✓ Hvor fleksible er alarm-mekanismene? Hvilke alternativer finnes for avlevering av alarmer av ulik alvorlighetsgrad?
- ✓ Er rapportgeneratoren tilstrekkelig fleksibel til å kunne generere rapporter med innhold og format som vi ønsker?
- ✓ Kan installasjon av programvareoppdateringer og nye konfigurasjoner automatiseres?

Sørg for å finne og prioritere de kravene som er viktigst i den foreliggende situasjon – som kan omfatte noen eller samtlige fra listen ovenfor, og andre i tillegg. Når vi har prioritert kravene i forhold til hverandre, har vi grunnlag for å sammenligne ulike produktalternativer – for eksempel i en tabelloppstilling (regneark):

Krav-kategori	Vekttall	Prod. 1	Prod. 2	Prod. 3
Skalerbarhet	50	4
Support	40	4
Sikkerhet/kryptering	25	3
Styringsmekanismer, enkelhet	20	2
Rapportgenerator	20	2
Alarm-avlevering	30	2
Signaturer (format, kilder, oppdateringsmekanismer)	20	3
...	??	
Sammenlagt		

Vekttallene som tilordnes, reflekterer våre prioriteringer og er utslagsgivende for resultatet, og må velges med omhu. Karakterene per produkt kan for eksempel skaleres fra 1-5 eller 0-10. En kortere skala gir enklere og ofte mer rettferdig evaluering.

Mens en slik oppstilling forenkler evalueringen, er det fortsatt optimalt å bruke sunn fornuft: Dersom referanser forteller at en leverandør ikke holder mål, spiller produktets karakteristika ingen rolle, og kan fjernes fra oppstillingen. Videre kan enkelte av kravene være av en slik art at dårlig karakter gjør de andre egenskapene uinteressante. Skalerbarhet er typisk et slikt krav.

Produkter

Tabellen nedenfor viser noen av de mest kjente leverandørene og produktene i segmentet, og er langt fra komplett. Segmentet er i høyeste grad dynamisk, preget av fusjoner, oppkjøp, overtagelser og nykommere, hvilket betyr at en slik oversikt går ut på dato etter kort tid. Å foreta aktive undersøkelser i markedet er derfor en nødvendighet.

Leverandør	Produkt	Type	Beskrivelse/kommentarer
Cisco www.cisco.com	Cisco IDS (tidligere NetRanger)	Aktiv NIDS, HIDS	En produktfamilie bestående av selvstendige, aktive NIDS-moduler og bokser, samt HIDS programvare på OEM-basis fra Enterscept.
Symantec www.symantec.com	Intruder Alert 3.6	HIDS	Programvarebasert aktiv beskyttelse av tjenerne for NT, W2k, Unix og Netware. Produktet kommer fra selskapet Axent, som ble overtatt av Symantec i 2001.
ISS (Internet Security Systems) www.iss.net			En omfattende samling programvareprodukter som dekker spekteret fra PCer til store nettverk, fra IDS til sikkerhetskontroll. Produktene kommer fra en håndfull ulike selskaper som er oppkjøpt av ISS i løpet av de siste årene.
Snort www.snort.org		NIDS/HIDS	Et populært <i>Open Source</i> innslag som er tilgjengelig på de fleste plattformer, inklusive W2k. Enkelt å sette i drift og egentlig et NIDS – dersom vertsmaskinen settes opp som en ruter.
Enterscept Security Technologies www.enterscept.com	Enterscept 2.5	HIDS	Programvare for aktiv beskyttelse av tjenerne. Selskapet kaller produktet et <i>Intrusion Prevention System</i> , og er ikke alene om å strekke definisjonene til et slikt nivå.
Tripwire www.tripwire.com www.tripwire.org		HIDS	Kommersielle Tripwire tilbyr flere HIDS-produkter for ulike sammenhenger, mens det opprinnelige <i>Open Source</i> produktet utvikles videre for Linux, og er gratis.
Enterasys Networks www.enterasys.com	Dragon	NIDS/HIDS	Programvaremoduler for HIDS og hardware-moduler for aktiv NIDS. Sistnevnte installeres i selskapets rutere og svitsjer.
OneSecure www.onesecure.com	IDP	NIDS	" <i>Intrusion Detection and Prevention</i> " (IDP) er hva OneSecure mener å levere. Systemet er implementert som en <i>black box</i> som installeres i tilknytning til en brannmur, og administreres via et eget verktøy.
NFR Security	NFR IMS (Intrusion Management System)	NIDS, HIDS	Aktiv NIDS gjennom spesialisert hardware, og programvaremoduler for HIDS tilpasset Windows, Solaris, AIX og HP-UX.
IntruVert www.intruvert.com	IntruShield	NIDS	Spesialisert hardware i flere ytelseskategorier opp til Gigabit Ethernet. Benyttes aktivt, passivt eller semi-aktivt gjennom indirekte styring av svitsjer.
MazuNetworks www.mazunetworks.com	DDoS Enforcer	NIDS	En familie av spesialiserte 'bokser' med ulik kapasitet for aktiv NIDS i mellomstore og store nettverk.
Counterpane Internet Security Guardent SecureWorks	Leverandører av IDS som tjeneste, typisk som en del av en såkalt <i>Managed Security Solution</i> , altså en <i>outsourcing</i> av hele sikkerhetsansvaret.		

Prosess

Når produkt(ene) er valgt, begynner det praktiske arbeidet, hvis omfang kan strekke seg fra installasjon av et par bokser til en prosess

NIDS – Network based Intrusion Detection System

HIDS – Host based Intrusion Detection System

Se avsnittet om kategorier i første artikkel, side 8 (Mellvik-Rapporten nr. 93).

DDoS – Distributed Denial of Service attack

som går over flere måneder. Prosessen fungerer omtrent som en overhaling av nettverket, og må gjennomføres i små trinn, slik at regulær drift ikke forstyrres.

Dersom hele nettverket skal sikres, har følgende rekkefølge i praksis vist seg å være optimal:

- ✓ NIDS i kanten av nettverket, i tilknytning til brannmurer.
- ✓ HIDS og eventuelt applikasjons-spesifikke alarmer på kritiske systemer som er tilgjengelige utenfra.
- ✓ HIDS og applikasjons-alarmer på kritiske interne tjenere.
- ✓ NIDS på viktige interne nettverk.
- ✓ HIDS og applikasjons-alarmer på sekundære interne tjenere.
- ✓ NIDS på resten av de interne nettverkene.
- ✓ HIDS på klienter.

Veien videre

Det er et faktum at de fleste av dagens IDS produkter lover mer enn de kan holde. Årsaken er ikke først og fremst tekniske eller designmessige svakheter i produktene, men at oppgaven er komplisert og at det er krevende å konfigurere produktene optimalt for en gitt situasjon og organisasjon. Denne utfordringen blir ikke mindre over tid, og aksentuerer behovet for å leie IT-sikkerhetstjenester – på samme måte som vi leier Securitas og andre for fysiske (tradisjonelle) sikkerhetstjenester.

Langt fra alle oppgaver er imidlertid store nok til å kvalifisere leie av tjenester på dette nivå. Mens sikkerhet er viktig i alle sammenhenger – fra gutterommet til styrerommet, er det også et faktum at verdien som skal eller bør beskyttes dekker et enormt spekter. Samtidig er det viktig å huske at det langt fra alltid er trusselen om tyveri som er den største. Hærverk og vandalisme kan være vel så aktuelt, spesielt i privatmarkedet. Dermed er det naturlig at det utvikler seg et spekter av tjenester og utstyr for beskyttelse – herunder IDS-systemer, som dekker spennvidden av behov. Alarmsystemer i hjemmet, bilen og på hytta er relativt enkle og rimelige – i anskaffelse og drift, og leverer den grad av trygghet vi betaler for. Tilsvarende funksjonalitet kommer på IT-området, der utstyret (bredbåndsrutere og lignende) etterhvert vil bli utstyrt med IDS-funksjonalitet som kan kobles opp mot kommersielle alarmtjenester betjent av eksperter.

At tjenesteleverandører i voksende grad overtar ansvaret for sikkerhet og alarmsystemer, betyr ikke at behovet for sofistikert utstyr blir mindre. Tvert imot fortsetter utviklingen av etterspørsel og produkter – et forhold som ikke minst kom til uttrykk på Networld+Interop i Las Vegas (se egen artikkel på side 4). Trenden går klart i retning av aktiv trafikkfiltrering i sann tid, såkalte 'aktive NIDS' – se første artikkel (Mellvik-Rapporten nr. 93 side 8). I sin streben etter å distingvere seg fra konkurrentene, kaller leverandørene gjerne slike systemer for 'Intrusion Prevention Systems', mens 'angreps-blokkering' er en langt

mer korrekt beskrivelse: Svakheterne er fortsatt de samme, men et aktivt IDS kan være i stand til å blokkere angrepet. Dette er en prestasjon av høy verdi i seg selv. Samtidig er det innlysende at eliminering av svakheterne som gjør inntrenging mulig, ville ha hevet sikkerhetsnivået enda et hakk.

Intrusion Prevention – en drøm?

Resonnementet bringer oss over til en ny form for – eller grad av – sikkerhet som kan oppnås gjennom ekte ‘innbrudds-avverging’ – immunisering om vi vil. Dagens IDS-systemer forteller en bedrøvelig historie om gjennomgående dårlig programvarekvalitet og slapp system-/nettverks-administrasjon, mens de sier lite om inntrengernes og angripernes dyktighet. En hel industri er skapt på grunnlag av markedets løpende aksept av elendig programvare fra leverandører som inntil nylig i beste fall har snakket pent om sikkerhet, men forøvrig ikke har brukt en kalori – eller krone – for å rette på forholdet.

Problemet blir ikke mindre med årene, tvert imot: Amerikanske CERT/CC rapporterer om en femdobling av innmeldte ‘hendelser’ fra 1999 til 2001. En del – men langt fra halvparten – av økningen kommer fra større grad av bevissthet i markedet, og voksende tro på at det hjelper å melde fra.

Behovet for å komme ut av dagens reaktive modus – innbruddsdeteksjon, og over til en proaktiv situasjon der innbrudd avverges, er åpenbar, men hvordan kommer vi dit? Resepten er enkel nok – på papiret: Programvare må kvalitetskontrolleres på en ganske annen måte enn hittil. Logiske feil, kodingsfeil, *buffer overruns* og utilsiktede hull er unødvendige – resultater av dårlig håndverk, manglende kvalitetskontroll, forhastede produktlanseringer og markedets manglende evne til å stille krav. At produkter av god kvalitet koster mer, er innlysende og akseptabelt. Sluttregningen blir mindre i alle fall dersom vi kan redusere sikkerhetstiltakene og fjerne IDS- og andre systemer.

Utfordringene er imidlertid ikke begrenset til programvare. Konfigurasjon – av operativsystemer, filsystemer, nettverksutstyr, klienter og så videre – representerer minst like store hull. Mens det er et akseptert prinsipp for god sikkerhet å sørge for at alt som ikke er eksplisitt tillatt, er forbudt, leveres de fleste systemer med oppsett etter det motsatte prinsipp. Overarbeidede eller inkompetente driftspersoner har verken tid eller kunnskap til å rette på forholdet. Igjen er det leverandørene som må gjøre en innsats for å bringe situasjonen under kontroll: God sikkerhet må bli en selvfølge, et ufravikelig krav, ikke en mulighet.

Selv etter en dramatisk bedring av kvaliteten på programvare, vil det imidlertid bli oppdaget svakheter: Feilfrihet finnes ikke, like lite som sikkerheten noen gang kan bli 100%. Det betyr at vi fortsatt vil leve med *patcher* og oppdateringer, og at leverandørene må øke innsatsen for å få disse ut til sine kunder og brukere. Lite hjelper det imidlertid at leverandørene blir bedre, dersom markedet ikke skjærper seg: Situa-

Microsoft skylder på inntrengerne

Microsofts Jim Allchin nyter stor faglig respekt for sine bidrag til Windows NT og 2000, men må ha mistet bakkekontakten da han nylig uttalte følgende til Information Week: *“I wouldn't say that we're any better or any worse than anyone else. I think it's a disservice to point fingers at us. ... I do believe that systems have worked just fine if they've not been under malicious attack. Malicious attacks don't have anything to do with quality, per se.”*

Dersom dette er representativt for substansen i Microsofts innsats for bedre sikkerhet, som ble slått stort opp for noen måneder siden, har vi lite å se frem til. Hvor langt ville Ford eller VW komme med argumentet: “Det er dårlige veier som har skylden. Bilene er av god kvalitet, de. At hjul og skjerm ramler av på dårlige veier har ingen ting med kvalitet å gjøre.”

CERT/CC – Computer Emergency Response Team/Coordination Center

sjonen i dag er at viktige sikkerhetsrelaterte oppdateringer blir liggende hos de samme driftsavdelingene vi nevnte ovenfor, og aldri benyttet. Slik skjødesløshet kan aldri gi god – eller tilfredsstillende – sikkerhet. Som vi har vært inne på tidligere i Mellvik-Rapporten, blir selv rudimentære sikkerhetstiltak – som innføring av aksesskontroll på filsystemer og i databaser – ofte ignorert, under påskudd av for lite tid. Resonnementet er omtrent like naivt som å si at vi ikke har tid til å puste.

Hvordan kommer vi så videre i retning mot *Intrusion Prevention* – og mot overflødiggjøringen av IDS-systemer? Det er i alle fall ingen grunn til å holde pusten. Så lenge vi – markedet – aksepterer dagens kvalitetsnivå, uteblir forbedringene. Det er et underlig tankekorst at vi forhandler frem flåteavtaler, serviceavtaler, tjenestenivåer og straffereaksjoner på alt fra biler og strøm til båndbredde og rekruttering, mens programvarekvalitet går for lut og kaldt vann, til tross for vår totale avhengighet. Markedet har latt seg lure av argumenter om at verktøy og systemer på død og liv må være enkle å bruke, ellers vil ikke brukerne ha dem, eller opplæringen blir kostbar. Men hva skal vi med brukervennlige systemer dersom de er usikre og ustabile?

Opplæring er ingen luksus, men en nødvendighet, og å tro at å spare på opplæringen gir gevinst i lengden, er å spare seg til fant. Hyllemeter (eller CD-samlinger) med dokumentasjon har liten verdi som annet enn oppslagsverk for spesialister som har fått skikkelig grunnopplæring og praksis. Dette er spesielt viktig for driftspersonalet, som ikke bare skal være spesialister, men også ha en faglig utvikling som skaper trivsel og interesse, og derigjennom stimulerer både til mer læring og til ekstra innsats når det trengs.

Langt lerret – høye mål – viktig realisme

Intrusion Prevention er som vaksine – i motsetning til antivirus-tiltak og IDS-systemer: Mens sistnevnte angriper et konkret problem, blir vaksinen en del av kroppens selvforsvar, og bygger opp immunitet mot gitte trusler. Tilsvarende gjør *Intrusion Prevention* våre systemer og nettverk resistente mot bestemte former for angrep og trusler.

Fremtidsvyene – eller drømmene, som noen utvilsomt vil kalle dem – forandrer ikke på det faktum at IDS-systemer er viktige og nødvendige ingredienser for god sikkerhet i dag – og i overskuelig fremtid. Det betyr at vi må ha et forhold til deres rolle, hvilke krav de skal tilfredsstillende og hvordan de brukes og holdes i drift. ■