

Innbruddsdeteksjon

Denne artikkelen er den første i en serie på tre om innbruddsdeteksjon, Intrusion Detection Systems (IDS).

Vi har installert brannmurer, filtre, demilitariserte soner, proxy-tjenere, autentisering, VPN-teknologi og virus-kontroll. Videre har vi brukt avanserte verktøy for å kontrollere sikkerheten, finne hull og svakheter, som siden er tettet og kontrollert på nytt. Like fullt må vi erkjenne at sikkerheten aldri kan bli 100%. Analogien med vår fysiske hverdag er slående: Låser, kontrollposter, portvakter, ID-kort og bagasje-skanning. Men hvor er innbruddsalarmen?

Vi vet av erfaring – fra blant annet hjemmet og bilen – at alarmsystemet er like viktig som låsemekanismene: For avskrekking – i den grad det er synlig, og for å avsløre tilfellene der innbruddet er et faktum. Hvorfor hører vi så lite om alarmsystemene i IT-sikkerhetssammenheng?

Nå er det innlysende at å avsløre innbrudd i nettverk og IT-systemer er krevende på et annet nivå enn for bil eller bolig. Hva skal vi se etter, hvor er symptomene og hvordan skal de håndteres? Heldigvis er det ytterst få av oss som har behov for å kunne svare på så detaljerte spørsmål. For oss andre er det viktigst å vite at slike alarmsystemer finnes, fungerer og er tilgjengelige – i en lang rekke klasser og kategorier, fra gratis (*Open Source*) programvare-overvåking til sofistikerte trafikk-prosessorer. Videre har vi behov for grunnleggende kunnskap knyttet til systemenes karakteristika, anvendelsesområder, nytteverdi og kompleksitet. Til sammen gir denne kunnskapen fundament for å ta steget til neste nivå av IT-sikkerhet.

Et overmodent behov

Årsaken til det akutte behovet for avanserte alarmsystemer er ikke at verden rundt oss er blitt mindre redelig eller mer ondsinnet, men at den er blitt større: Hele verden passerer daglig forbi vår dørstokk, og stadig flere av oss er avhengige av at flest mulig av de forbigående stikker innom for å se hva vi har å tilby, kanskje sågar gjøre en liten eller stor handel. Forholdene ligger godt til rette for 'nasking' – i overført betydning, utført av kunder eller interne brukere.

Dermed bringes tankene over på butikk-systemer der varene er merket med brikker, slik at alarmen går dersom de tas ut av lokalet uten å være sjekket i kassen. Video-overvåkingssystemer bidrar til ytterligere sikring gjennom kontinuerlig monitorering av bevegelsene i lokalet.

Sikkerhet – mer enn forsvar

Situasjonen – og behovet – er analogt på IT-siden: Truslene er å finne eksternt og internt, og fordrer avanserte overvåkings- og alarmsystemer for å kunne bringes under kontroll. De ønskede egenskapene i slike alarmer – IDS, *Intrusion Detection Systems* på fagspråket, er

enkle: De skal rapportere mistenkelige eller uønskede hendelser til den eller de ansvarlige – med

- ✓ 100% pålitelighet og nøyaktighet,
- ✓ uten opphold – i praksis på mindre enn 1 minutt,
- ✓ med kortfattet, men fyllestgjørende beskrivelse av situasjonen,
- ✓ og en anbefaling med hensyn til hva som bør gjøres.

At produkter som kan tilfredsstille alle disse kravene neppe finnes, er kanskje innlysende. På den andre siden er det et faktum at overvåkingssystemer – med varierende grad av omfang og kvalitet – har eksistert siden 60-tallet, spesielt i bank- og finans-miljøer. Vi står med andre ord ikke overfor et nytt fagfelt som trenger lang modningstid for å finne sin faglige og kommersielle plass i en overbefolket virkelighet. Verden har riktignok forandret seg dramatisk siden de første overvåkingssystemene trådte sine barnesko, og dagens trusselbilder har lite til felles med historien. Likeledes har produktene få egenskaper som minner om deres tidligste forfedre. Ikke desto mindre står vi overfor problemstillinger og tilhørende teknologi som har hatt lang modningstid, og som burde være i stand til å dekke våre behov. Hvor nær opp til målsettingen er det mulig å komme og til hvilken pris?

I tre artikler skal vi gjennomgå den virkelighet vi står overfor – trusler og behov, metoder og løsninger, produkter og alternativer, forventninger og realiteter.

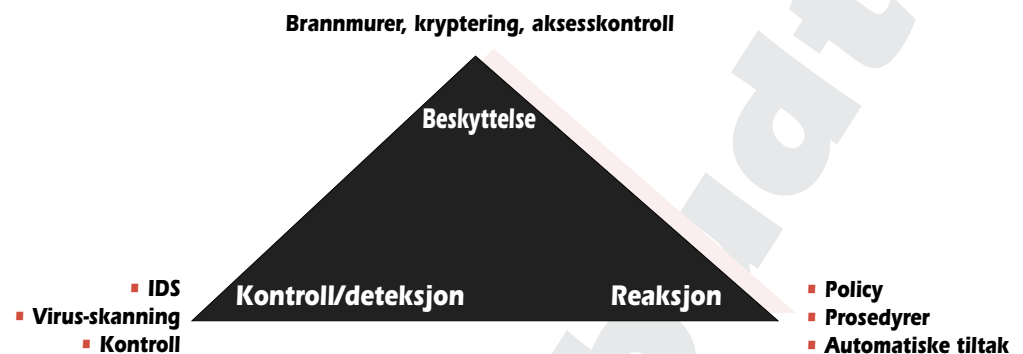
Fra begrep til løsning

Er denne innledningen slik å forstå at IDS er et produkt – som kan bestilles og betales? Det finnes en lang rekke produkter, kommersielle såvel som frie, som kaller seg IDS: Markedsføringen forteller at med produkt XX kan vi endelig føle oss trygge – men hvor effektive er de ulike produktene, hva skiller dem og hvordan er nytteverdien når ulykken først er ute?

Eller beskriver begrepet IDS egentlig en prosess – det å overvåke trafikk, loggfiler eller lignende på søken etter uvanlige innslag eller mønstre? Hva er det i så fall viktig å kontrollere, og hvordan skiller vi støy fra relevant informasjon?

Sist, men ikke minst: Er IDS virkelig løsningen på alle våre gjenværende sikkerhetsproblemer? Hvis vi alltid kan oppdage innbrudd og uvedkommende, er det da nødvendig å låse døren? Kan vi droppe andre sikkerhetstiltak? Er opplæring og bevisstgjøring av brukerne ikke lenger påkrevet?

Svaret gir seg selv, men forvirringen er like fullt stor: På samme måte som sikkerhet generelt, er også IDS en prosess. Produkter – det være seg hardware, programvare eller kombinasjoner, er nødvendige, men langt fra tilstrekkelige elementer i prosessen.



Figur 1 God sikkerhet fundamenteres på en rekke individuelle elementer som gjerne grupperes i tre hovedgrupper – en trekant-symbiose.

Delene – og helheten

På samme måte er et alarmsystem, som vi heretter kaller et IDS, ett av en rekke viktige elementer i en total sikkerhetsløsning. Elementene grupperes gjerne i tre hovedgrupper – et trekantforhold som er illustrert i figur 1. Slike 'treenigheter' er sjelden i balanse. Vekten – tyngdepunktet – har en tendens til å trekke ut mot én av 'armene' i trekanten på bekostning av de andre.

I vår sammenheng er det praktisk talt uten unntak beskyttelse som får størst oppmerksomhet. Brannmur, filtre, krypteringsmekanismer og VPN hører hjemme her, og fortjener oppmerksomhet, men ikke på bekostning av de andre. I og med at perfekt beskyttelse ikke er mulig, blir en ensidig fokusering på nettopp beskyttelse, meningsløs.

Risikoer finnes over alt, og gjennom ti år med Internettet rundt oss på alle kanter, har vi lært at dets eksistens og vår tilknytning dertil, representerer et nytt trusselnivå med hensyn til IT-sikkerhet. Alarmer, kontroll og deteksjonsmekanismer er vårt svar på denne eskaleringen av risikoer – det er her vi styrer vårt risikonivå: Med IDS-systemer, virus-kontroll og andre kontrollmekanismer.

Den tredje og siste armen i vår trekant, er beredskap: Hvordan reagerer vi når forsvaret er forsert, og deteksjonsmekanismene sender en alarm? Hvilke virkemidler har vi til rådighet og hvordan bruker vi dem? Enkelte produkter skryter av at de kan sette i verk tiltak automatisk, men den generelle regelen er fortsatt at mennesker må til – for å evaluere signalene og iverksette riktige tiltak. På grunnlag av etablerte regler og prosedyrer, kan den eller de ansvarlige håndtere situasjonen på en måte som er optimal for organisasjonen. Automatiske tiltak er mulige i enkle og oversiktlige situasjoner – dersom utstyret er tilstrekkelig sofistikert, et forhold vi skal komme tilbake til.

Kontroll og deteksjon

Den skjeve tyngdefordelingen i vår sikkerhetstrekanter fører til at både kontroll-tiltak og planer for håndtering av innbrudd ofte mangler eller er mangelfulle. Situasjonen er på den ene siden utilfredsstillende og på

den andre siden naturlig: Selv i 2002 blir sikkerhet ofte betraktet som et produkt, for eksempel en brannmur: Når den er på plass, er sikkerheten ivaretatt. Skrekkeeksemplet i den forbindelse er et søramerikansk universitet som gikk til anskaffelse av en brannmur, plasserte den i et rack ved siden av nettverksforbindelsene, og lot den stå. Strømmen ble aldri slått på og ingen kabler koblet til.¹

Mens fysisk beskyttelse er konkret og lett å forholde seg til, er definisjonene langt mer vage og uklare i forbindelse med deteksjon og kontroll: Hva er et 'innbrudd', hvor går grensene, hva skal til for at vi kan si at forsvaret er 'penetrert'? Likeledes er det innlysende at alarmer og deteksjon er lite verdt dersom ingen reagerer når alarmen går. Det betyr ikke at enhver alarmsituasjon krever umiddelbar oppmerksomhet fra en ansvarshavende person, men at vedkommende blir gjort kjent med situasjonen og får anledning til å vurdere hvilke tiltak som er optimale.

I enkelte tilfeller kan beskyttelse og deteksjon utfylle hverandre. For eksempel forekommer det at bevisste hull etableres – midlertidig eller permanent – i forsvarstiltakene, for å ivareta spesielle behov. Den risiko dette alltid medfører kan reduseres ved å skjerpe oppmerksomheten rettet mot nettopp denne trafikken – å heve nivået for overvåking og kontroll.

Metoder og mekanismer

Å oppdage forandringer er en sentral egenskap i ethvert alarmsystem, uansett sammenheng. Videre er det viktig å kunne filtrere 'observasjonene' slik at naturlige eller tillatte forandringer elimineres, mens de ureglementerte analyseres og flagges. For eksempel vil et videobasert utendørs overvåkingssystem måtte skille mellom grener og gress som beveger seg i vinden, biler eller husdyr som sporadisk passerer og alminnelig inn/ut-trafikk på den ene siden, og mistenkelige person- eller kjøretøy-bevegelser på den andre.

Prosessen blir ikke enklere når vi flytter oss til IT-systemer, der vi skiller mellom tre metoder som hver på sin måte søker etter mistenkelige forandringer:

- ✓ **Signatur-analyse:** Datasamlinger (filer) eller -strømmer analyseres innholdsmessig på søken etter mønstre som er kjente eller mistenkelige. Metoden forutsetter at truslene er kjente, og virker åpenbart ikke på nye eller endrede trusler (dvs. nye signaturer). Virus-skannere fungerer etter dette prinsippet, og de fleste IDS-systemer har mer eller mindre avanserte mekanismer for slik signatur-analyse.
- ✓ **Protokoll-analyse:** Datastrømmer på nettverket analyseres i sann tid for å finne mistenkelige mønstre. Her er spennvid-

¹ Historien forteller mer om mangelfull kommunikasjon enn om manglende kunnskap: IT-ansvarlige visste naturligvis godt at brannmuren hadde null verdi der den sto, mens de bevilgende og formodentlig ansvarlige myndigheter sto for anskaffelse av enheten og kunne toe sine hender med hensyn til sikkerhet. At de samtidig hadde 'glemt' å sette av penger til installasjon, opplæring og vedlikehold, påvirket åpenbart ikke trygghetsfølelsen.

den stor: Hyppige forekomster av protokoller som normalt er sjeldne, aksess til porter som ikke er i bruk – eller dybde-kontroll av hver enkelt pakke, som kan avsløre angrep på spesielle applikasjoner eller forsøk på utnyttelse av kjente svakheter.

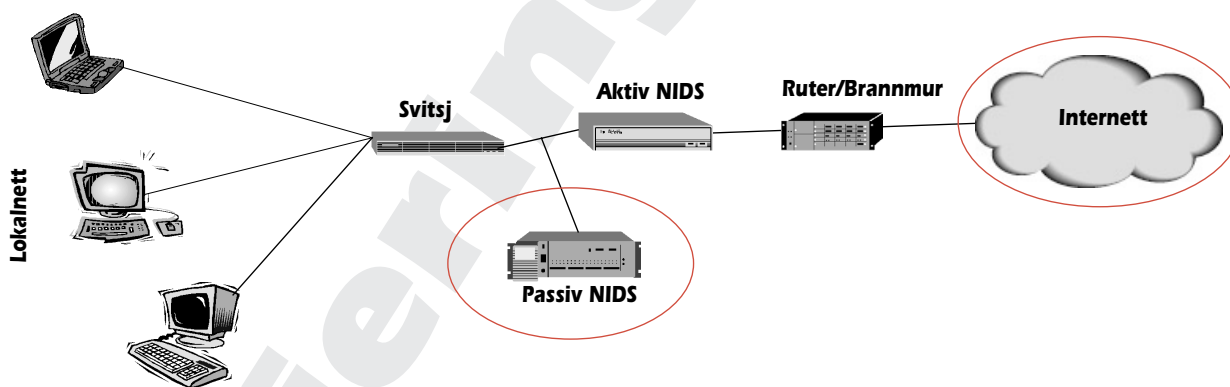
- ✓ **Avviksdeteksjon:** Den mest kompliserte metoden for IDS, og den mest lovende. Her benyttes avansert statistisk modellering av det normale – trafikk eller data, som så legges til grunn for løpende sammenligninger. En kombinasjon av statistiske metoder og kunstig intelligens behandler dataene, og bygger opp erfaring samtidig med at det søkes etter mistenkelige mønstre eller forandringer. Det finnes også enkle og lett detekterbare avvik som kan gi viktige indikasjoner på at noe er i gjære. For eksempel vil en navnetjener-forespørsel til en maskin som ikke har en slik tjeneste og aldri har hatt det, være mistenkelig. Likeledes er det naturlig at en 'gammel' bruker som for første gang aksesserer et dataområde, forårsaker hevede øyenbryn.

Kategorier

IDS-systemer havner som regel i én av to hovedkategorier: Nettverksbaserte (NIDS), som arbeider direkte på datastrømmen på nettet, og vertsbaserte (HIDS), som kjører på og kontrollerer den enkelte maskin, enten det er en klient eller en tjener. Sistnevnte arbeider med data fra loggfiler som genereres av operativsystemet og lokale tjenester/applikasjoner.

HIDS – Host based Intrusion
Detection Systems

NIDS – Network based Intrusion
Detection Systems



Figur 2 En nettverksbasert IDS-boks kan settes IN-LINE i nettverket, som gir den mulighet til å aktivt styre trafikken dersom den oppdager 'uhumskheter'. Samtidig setter en slik plassering meget store krav til ytelse og kapasitet, hvilket medfører at slike produkter fortsatt er relativt sjeldne.

De nettverksbaserte systemene forekommer enten som rene programvareprodukter som installeres på generelle systemer, eller som spesialiserte bokser ('appliances') med varierende kapasitet og egenskaper forøvrig. Den passive varianten henges på nettverket som en hvilken som helst annen node (se figur 2). Den analyserer kontinuerlig datastrømmen, og har den åpenbare fordel at den ikke vil fungere som flaskehals dersom trafikken skulle bli for stor og den får for mye å gjøre.

Samtidig har den kun indirekte mulighet til å påvirke datastrømmen automatisk.

Den aktive varianten sitter som et filter 'midt i trafikken', hvilket stiller enorme krav til kapasitet. Samtidig ser vi at mulighetene i dette tilfellet er gode for å kunne (for eksempel) strupe en trafikkstrøm som ansees å være mistenkelig.

Tabell 1 Fordeler og ulemper knyttet til henholdsvis vertsbaserte (HIDS) og nettverksbaserte (NIDS) IDS-systemer.

Kategori	Fordeler	Ulemper
HIDS	Høy informasjonskvalitet: Genereringen av loggfiler kan i mange tilfeller styres, slik at vi får ut den informasjonen som trengs, og fjerner støy.	Høy systemavhengighet: Loggfiler er systemspesifikke, og et gitt verktøy dekker sjelden mer enn 2 eller 3 plattformer. Data som skal sendes til et 'sentralisert mottak' må normaliseres (standardiseres).
	Høy informasjonstetthet: Tilpassning (ovenfor) sammen med muligheten til å kombinere informasjon fra flere forskjellige logger, gjør det mulig å se sammenhenger og reduserer sjansene for at en inntrenger skal kunne gjemme seg effektivt.	Ytelse er en joker: Hvor mye ressurser krever IDS-systemet? Vil det forstyrre den vanlige driften? I så fall må vi benytte dedikerte maskiner som samler inn data fra flere kilder og behandler dem utenfor datastrømmen.
		Systemer er ofte angrepsmål i seg selv: Det betyr blant annet at loggfiler ikke nødvendigvis er å stole på, eller at IDS-systemet kan bli satt ut av drift.
NIDS (passive)	Ytelse: Ingen ytelsesmessige konsekvenser for berørte systemer og nettverk, vil overleve selv alvorlige DENIAL OF SERVICE angrep.	Ytelsesmessig krevende: Pakker kan gå tapt på tungt belastede nettverk.
	Robust mot 'fikling': En NIDS-boks kan gjøres fullstendig utilgjengelig fra nettverket.	Dekker sjelden alle tenkelige applikasjonsprotokoller, for eksempel SMB/Net-BIOS. Likeledes vil en del 'gamle' applikasjons- og system-protokoller gjerne være ukjente [produktene er normalt IP-sentriske].
	Administrasjon: Én boks å styre i stedet for en rekke systemer (som tilfellet er med HIDS).	Kryptering: Krypterte datastrømmer kan ikke kontrolleres [denne utfordringen kan løses ved å plassere IDS-systemet annerledes i nettverket, eller introdusere proxy'er som dekrypterer datastrømmen før den når sin endelige destinasjon].
	Generell: Beskjeden eller ingen plattformavhengighet (OS). Kan samle informasjonstyper som ikke vil finnes i loggfiler (f.eks. port-skanning og fragmentering).	

Aktive NIDS har omtrent de samme karakteristika som passive i denne sammenhengen, med unntak av ytelse, som vi var inne på tidligere.

I gruppen vertsbaserte systemer finner vi også enklere varianter med spesifikke, begrensede oppgaver:

- ✓ Filkontrollører – som regelmessig gjennomgår en gitt samling filer og kontrollerer (via avanserte sjekksum-algoritmer) at de ikke er forandret.
- ✓ Antivirus-programmer

- ✓ 'Honningkrukker' (agn, åte, *honeypots*) – fiktive samlinger av filer og tjenester opprettet for å trekke til seg oppmerksomheten fra uønskede besøkende.

Verts-baserte og nettverksbaserte systemer har hver på sin kant fordeler og ulemper, og dekker ulike, men delvis overlappende behov. Tabellen ovenfor gir en kortfattet oversikt over de viktigste egenskapene på begge sider av vektsskålen.

Vi skal i en senere artikkel se at mange av dagens produkter er hybrider, de kombinerer elementer fra både NIDS og HIDS. For eksempel kan en NIDS introduseres som en del av IP-stakken på en tjener, der den kontrollerer inn- og utgående trafikk for nettopp dette systemet, uten å bry seg om andre. Fordelene og ulempene med en slik variant er innlysende ut fra tabellen ovenfor.

Myter og realiteter

Oppstillingen av fordeler og ulemper i tabell 1 viser at IDS-systemer primært handler om teknologi – effektive kombinasjoner av programvare og hardware der ytelse er én av parametrene, mens intelligent behandling av data er like viktig. Systemet skal ikke bare få med seg alt, men samtidig kunne analysere, vurdere og trekke konklusjoner.

På samme måte som vi sier at 'det er menneskelig å feile', er det praktisk talt umulig å lage alarmsystemer som aldri gir falske alarmer. 100% treff og 0% falske alarmer er umulig, og vi blir alltid stående overfor et valg om hvor grensen skal gå: Skal vi ta sjansen på enkelte falske alarmer for å redusere muligheten for at noe slipper forbi uoppdaget?

Falske alarmer er en stor utfordring i forbindelse med de aller fleste IDS-systemer: De konsumerer ressurser – på systemsiden og personell-siden, og reduserer fokus på den egentlige oppgaven. Samtidig er det viktig å se skogen for trær: Falske alarmer er ille, men kan reduseres gjennom erfaring – aktiv bruk av data og signaturer som forårsaker alarmene. Over tid skal hyppigheten gå ned og etterhvert bli praktisk talt borte.

Innstillingen at falske alarmer er et problem, er med andre ord feil – og farlig. Fokus skal i stedet være rettet mot å unngå det som kalles '*false negatives*', altså situasjoner som ikke oppdages, men som burde ha blitt det. Likeledes er det en misforståelse at IDS-systemer kan avsløre misbruk av ressurser fra ansattes side. Følgende to punkter setter fokus på disse misforståelsene og henleder oppmerksomheten dit den hører hjemme:

- ✓ Myte: "Falske alarmer er et stort problem". Realitet: De virkelige problemene – som fortjener vår oppmerksomhet – er 'falske negativer' (situasjoner som går oss hus forbi), og underbemannede sikkerhets/drifts-grupper. Falske alarmer er håndterbare og må håndteres.

- ✓ Myte: “IDS-systemer kan avsløre misbruk”. Realiteten er at IDS-systemer detekterer problemer og avvikende (unormal) bruk. Misbruk avsløres av drifts- og sikkerhets-personell.

Neste utgave

I neste utgave skal vi blant annet diskutere hvordan smarte inntrengere (mennesker såvel som programmer) gjør seg flid med å unngå eller lure IDS-systemene. Vi skal også se nærmere på hvordan systemene fungerer i praksis.

I tredje artikkel (Mellvik-Rapporten nr. 95), tar vi frem en del produkt-eksempler og ser på deres karakteristika, hvor de passer inn, og hva som finnes på beddingen i nær fremtid. ■

Fersk litteratur

En høyaktuell bok som tar for seg nettopp IDS, og ført i pennen av verdens fremste eksperter på området, har tittelen

NETWORK INTRUSION DETECTION – An Analyst’s Handbook (2nd ed.) av Stephen Northcutt og Judy Novak (New Riders Publishing 2002, ISBN 0-7357-1008-2).