



Använder obehöriga
ditt WLAN?

LANeye 2.3

Ett program som gör

Intrångsövervakning i nätverk

enkelt nog för vanliga användare.

Hindra obehöriga att ansluta till ditt nätverk!

LANeye övervakar nätverket genom att avlyssna nätverkstrafiken.

Om en ny okänd dator försöker ansluta till nätverket upptäcker LANeye det omedelbart.

LANeye larmar och nekar den anslutande datorn tillgång till nätverket.






Du bestämmer själv om du vill godkänna datorn på ditt nät.

LANeye - En helt ny typ av nätverksskydd.

<http://www.proprat.se>

<http://www.laneye.se>

LANeye skyddar ditt nätverk från intrång i tre steg.

Detekterar	Larmar	Blockerar
 <p>LANeye upptäcker om obehöriga datorer försöker ansluta till ditt nätverk eller WLAN.</p>	 <p>LANeye larmar och loggar incidenter</p>	 <p>LANeye hindrar anslutande datorer tillgång till andra datorer, utdelade filer och skrivare på ditt nätverk.</p>
 <p>LANeye upptäcker om behöriga datorer betar sig misstänkt när de ansluter till ditt nätverk eller WLAN.</p>		 <p>LANeye hindrar anslutande datorer tillgång till en giltig IP-adress på ditt nätverk.</p>

Använder obehöriga ditt WLAN?

Med LANeye har du full kontroll över vilka enheter som ansluts till ditt nät. LANeye detekterar inte bara datorer. LANeye ser dina nätverkskrivare, routrar, WLAN punkter, servrar. Ja alla enheter som kommunicerar på ditt nät upptäcker LANeye.

I LANeye klassar du dina nätverksenheter som kända. När en ny enhet försöker ansluta sig lägger LANeye den till en lista över okända enheter. Okända enheter blockeras tillgång till nätverket. Om du vill tillåta den nya enheten flyttar du den i LANeye till en lista över kända och tillåtna enheter.

LANeye är inte en brandvägg.

LANeye fungerar på ett helt annat sätt än hur en brandvägg fungerar. LANeye hindrar inte trafiken på ditt nätverk utan istället avlyssnas trafiken. När LANeye blockerar en anslutande dator lägger sig LANeye i anslutningsförfarandet och skickar nekande datapaket till den inträngande datorn. Det gör att LANeye även bevakar att din brandvägg gör sitt jobb.

LANeye kan köras på valfri dator.

Detektering och blockering fungerar lika bra oavsett på vilken dator i nätverket som LANeye körs på.

LANeye använder inga koder, ingen kryptering, inga lösenord.

LANeye använder sig bara av nätverkets fundamentala byggstenar för att skydda ditt nätverk.

Hot mot säkerheten kommer inte bara utifrån. I ett företagsnät är det inre hotet oftast större än det yttre. Medarbetar utan illvilligt uppsåt kan lätt äventyra säkerheten när bärbara datorer blir vanligare.

Ställ dig följande frågor:

- Tillåter företaget där du är verksam att medarbetare använder sin bärbara dator hemma?
- Används bärbara företagsdatorer på publika nätverk när medarbetare är ute och reser?

Säkerheten i andras nätverk känner man inte till. När man varit på ett annat nät skall man tänka på att:

- Inloggningsförfaranden kan ha snappats upp.
- Säkerhetsluckor kan ha utnyttjats för att plantera in skadlig kod.
- Säkerheten i hemnätverk är generellt sett betydligt lägre än i företagets nätverk.

LANeye detekterar skiljande anslutningsförsök. Det blir allt vanligare att obehöriga som vill komma åt andras nätverk försöker imitera (låtsas vara) en av nätverkets kända och tillåtna datorer. LANeye kan avslöja om en dator har varit på ett annat nätverk när den försöker ansluta till det egna nätverket. Funktionen i LANeye kallas kapningsvarning och när det detekteras så nekas även en känd dator anslutning till nätverket. Den här funktionen kan användas för att hindra anställda att ansluta sin bärbara datorn efter att den använts på användarens eget hemnätverk.

- **Använd LANeye** för att hindra datorer som varit på ett annat nät än det egna, att ansluta till ditt nätverk.

Hur fungerar LANeye?

När datorer ska kommunicera med varandra på ett nätverk skickas informationen ut lite på måfå skulle man kunna säga.

Alla datorer har en anslutning till nätverket. Det en dator skickar ut när alla de övriga datorerna.

För att de olika datorena skall se skillnad på varandra har varje dator ett unikt ID kallat MAC-adress (Media Access Control adress). MAC-adressen är knuten till hårdvara och ska inte förväxlas med IP-adresser. MAC-adressen används av datorerna för att dom ska slippa ta emot all trafik och bara ta emot trafik som är ämnad dom själva.

När en dator pratar med en annan dator på nätverket skickar den sändande datorn ut sin MAC-adress och MAC-adressen till den mottagande datorn. På så sätt ser den mottagande datorn att det som kommer är ämnat för den och den ser också från vem det kom så att ett svar kan skickas tillbaka till rätt dator.

Nu säger den vakne nätverksteknikern att nätverkstrafiken sprider sig inte till samtliga datorer i nätverket eftersom man använder switchar som på ett intelligent sätt minimerar trafiken i olika segment i nätverket. Switchen vet vilka datorer som finns i det egna segmentet och skickar inte ut trafik som inte hör hemma där. Detta är helt riktigt, nästan.

När en dator ansluter sig till nätverket skickar den ut så kallade broadcast meddelanden, ett slags all-anrop. Den anslutande datorn gör det för att de övriga datorerna ska känna till att den kommit in på nätverket. Dessa all-anrop förmedlar switcharna vidare i samtliga segment och det räcker för att LANeye skall upptäcka den nya datorn.

Innan den anslutande datorn kan börja kommunicera på nätverket måste den förhandla med de övriga datorerna.

Med olika all-anrop önskar sig den anslutande datorn ett föreslaget namn, IP adress, arbetsgrupp, domän mm. Om datorn som ansluter sig inte är önskvärd i nätet skickar LANeye nekande datapaket till den anslutande datorn som säger att de önskade adresserna och namnen inte är tillåtna på nätverket. Utan namn och adress kan den inte vara med på nätverket.

Oftast leder detta till att den inträngande datorn gör omförsök, frågar på nytt. LANeye fortsätter då att skicka nekanden tills om du väljer att ta bort blockeringen i LANeye.

LANeye skickar bara nekanden under förhandlingsfasen när en dator ansluter sig. Det betyder att datorer som redan finns på nätverket inte "kastats" ut av LANeye.

Fallstudie 2

Ofta tänker sig inte människor för. På ett mindre företag hade en av medarbetarna en dag tagit med sig sin trådlösa accesspunkt han använder i hemmet till jobbet. Medarbetare ställde upp access punkten på fönsterbrädan i lunchrummet och kopplade in den till nätverket. För att dölja sin tilltag drog denne för gardinen så WLAN punkten inte var synlig. Allt för att kunna sitta och arbeta och dricka kaffe i en trevligare miljö. LANeye detekterade omedelbart att en ny enhet börjat kommunicera på nätverket av fabrikat D-LINK. Efter några minuter dök ytterligare en ny okänd enhet upp, Den lika så av fabriken D-LINK. LANeye identifierade att detta rörde sig om medarbetarens dator. Medarbetaren återfanns i lunchrummet sittandes arbeta och blev väldigt överaskad att man upptäckt tilltaget så snabbt.

Vad säger denna historia oss?

Det rörde sig inte om något egentligt intrång utan en obetänksam medarbetare. Historien förtäljer inte om företaget haft en IT-policy som medarbetaren inte förstått eller hade liten förståelse för eller om det rörde sig om ren obetänksamhet men bara det faktum att medarbetaren dolt WLAN punkten bakom gardinen säger ändå att denne hoppats på att tilltaget inte skulle uppdagas. Hade tilltaget inte upptäckts och WLAN accesspunkten stått kvar och varit aktiv skulle detta inneburit en ökad risk för intrång utifrån.

Mer information om LANeye hittar du på:
<http://www.proprat.se>
<http://www.laneye.se>

Programbeskrivning

LANeye lyssnar på nätverkstrafiken. Programmet startas varje gång man startar datorn och arbetar i bakgrunden. Information som LANeye samlar på sig om nätverkets olika enheter lagras i en så kallad omgivningsfil.

I programmets huvudvy ser man vilka bevakningsfunktioner som är aktiverade.

Larm visas visuellt i form av en trafikskylt men larm kan också skickas med epost till valfria epostadresser.

LANeye's huvudfönster är delat i två huvudsakliga vyer. Till vänster presenteras samtliga påträffade nätverksenheter i en trädvy. Till höger presenteras detaljer beroende på vilken nod i trädvyn man väljer.

Nätverksövervakning		Aktiverad
Intrångsdetektering		
<input checked="" type="checkbox"/>	Detektera nya okända datorer	Aktiverad
<input checked="" type="checkbox"/>	Detektera kapning av kända MAC-adresser	Aktiverad
<input checked="" type="checkbox"/>	Detektera misstänkta påloggningsförsök	Aktiverad
Intrångsblockering		
<input checked="" type="checkbox"/>	Blockera tillgång till nätverket	Aktiverad
<input checked="" type="checkbox"/>	Blockera IP-adress tilldelning	Aktiverad

The screenshot shows the LANeye application window titled "LANeye - Aktiverad Omgivning: Mitt nätverk". The interface includes a menu bar (Arkiv, Visa, Verktyg, Hjälp) and a toolbar with buttons for "Aktivera", "Avaktivera", "Ny", and "Hjälp". The main area is divided into two panes. The left pane, "Nätverksanslutningar", shows a tree view of network connections under "LAN", including "Kända Datorer" (with sub-items like DENNA DATOR, ZyWALL 5, Dator 2, Dator 1, PRNsrv) and "OKÄNDA Datorer" (with sub-items like {D-Link Corporation}, TLT-W2K, WA12). The right pane displays a table of network devices with columns for "Namn", "Senast Aktiv", and "IP Nummer".

Namn	Senast Aktiv	IP Nummer
\\ {D-Link Cor...	2006-03-05 10:13:39	* 172.16.1.2
\\TLT-W2K	2006-02-13 01:33:09	* 172.16.1.10
\\WA12	2006-02-19 21:17:44	* 172.16.1.10

At the bottom of the window, there are status indicators: a green leaf icon with "= 5 (3)", a red question mark icon with "= 3 (0)", a "CPU %" gauge, and a "LAN %" gauge showing "0 bytes/s".

Trädvyns nod "Okända datorer" visas de nätverksenheter som LANeye hittat (upptäcker) och som ännu inte identifierats av dig som administrerar LANeye. Här listar LANeye automatiskt alla nypåträffade nätverksenheter. Varningsymboler visar om ett intrång detekterats och om blockering av enheten är påslagen.

Trädvyns nod "Kända Datorer" listar de nätverksenheter som man valt LANeye identifiera som kända. De kända enheterna bevakas med kapningsdetektering och detektering av misstänkta påloggningsförsök. Enheter som ligger på listan över kända enheter kan också blockeras om de uppträder avvikande.

Listvyn till höger visar ett flertal kolumner med information som samlats in om noden. Med högerklick på en enhet kommer man åt enhetens egenskaper. En känd enhet kan typbestämmas till skrivare, gateway, trådlös accesspunkt mm. I egenskapsdialogen kan man också välja att manuellt slå på blockering för en viss enhet för att hindra den från att ansluta vid nästa anslutningsförsök.

Det går att flytta okända och kända datorer mellan listorna. Flyttar man en enhet från okända listan till listan över kända datorer så tas blockeringen automatiskt bort.

Incidenter loggas då LANeye detekterar intrång och blockerar. För varje enhet finns en incidentlogg. För varje händelse i loggen finns en beskrivning på vad som orsakat händelsen. Händelser lagras som meddelanden och olästa meddelande visas med fet stil.

Loggade händelser	Beskrivning	Tidpunkt
Dagens händelser = 3 (2)		
Blockering startad	Blockering startade för att hindra enheten från ...	2006-03-05 10:31
Enhetsinställning ändrad...	Varningsymbolen för denna enhet aktiverades f...	2006-03-05 10:23
Enhetsinställning ändrad av an...	Denna enhet flyttades av användaren från känd till okänd.	2006-03-05 10:18:50
Gårdagens händelser = 0 (0)		

Beskrivning av händelsen tar upp vad som kan vara troliga orsaker till att LANeye reagerade.

Orsak till incidenten

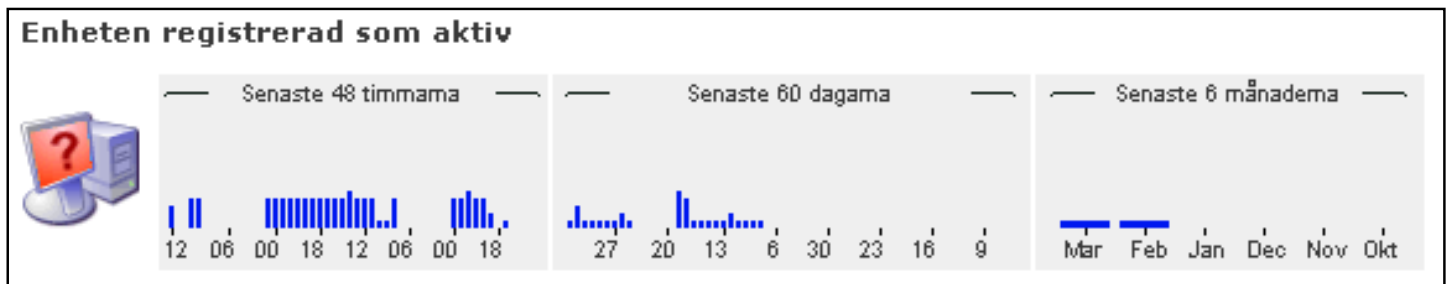
Denna intrångsincident kan ha orsakats av naturliga skäl såsom:

- Om en ny dator medvetet anslutits till nätverket.
- Om en ny annan enhet såsom en skrivare, router mm medvetet anslutits till nätverket.
- Om man nyligen installerat LANeye kan det finnas enheter som ännu inte gett sig till känna.

Denna intrångsincident kan också ha orsakats av:

- Att en främmande dator har anslutits till en av nätverkets WLAN punkter.
- Att en främmande dator har anslutits till nätverket via kabel.

Statistik över enheten samlas och visas som grafer över aktivitet. LANeye visar information om hur mycket och ofta en enhet är eller har varit aktiv. Statistik över intrångsdetekteringar och blockeringar visas på samma sätt.



Driftsättning av LANeye görs med hjälp av en guide. I guiden anger du vilket nätverkskort som LANeye skall använda och därefter gör guiden en undersökning av ditt nätverk. När guiden är klar har LANeye listat dina nätverksenheter som "okända" och du kan då gå igenom dessa och sätt enheterna som kända.

LANeye produktvarianter

LANeye 2.3 finns i två varianter.

LANeye 2.3 Small Network Edition är en version för fåmansföretagsnätverk och hemnätverk. Small Network Edition är enklare att handha. Den har alla bevakningsfunktioner men saknas vissa mer avancerade funktioner.

- För nätverk med upp till 10st enheter. (MAX 25 enheter kan hanteras).

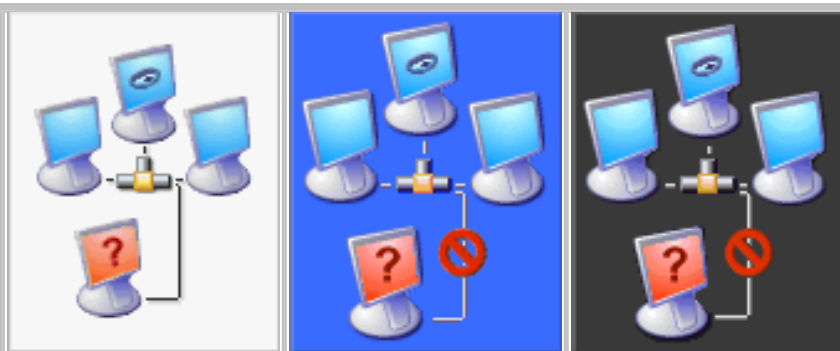
LANeye 2.3 Professional Edition är menad för större nät och nät med avancerade nätverksfunktioner och avancerade klienter.

- Klara stora nätverk.
- Exkluderingsfilter för VPN tunnlar / SAN (Storage Area Network) / Virtuella maskiner såsom VMware mm.
- Exkluderingsfilter för tillåtna IP-adress som tillåter användning av bärbara datorer i andra nät än det egna.
- Stöd för flera omgivningar för nät med flera logiska segment.

LANeye Produktvariantmatrix

Här se du skillnaderna mellan de olika varianterna av LANeye 2.3.

Version 1.6 visas för dig som redan använder en äldre version av LANeye.



Produktversionsnamn	LANeye 1.6	LANeye 2.3 Small Network Edition	LANeye 2.3 Professional Edition
Detektering av nya okända datorer	✓	✓	✓
Detektering av misstänkt MAC-adress kapning	-	✓	✓
Detektering av misstänkta pålogningar	-	✓	✓
Blockera tillgång till nätverket	-	✓	✓
Blockera IP-adress tilldelning	-	✓	✓
Lokalt larm	✓	✓	✓
Larm via E-post	✓	✓	✓
Trafiklogg	✓	✓	✓
Trafiklogg till skrivare	✓	-	-
Detaljerad enhetsinformation	-	✓	✓
Statistik	-	✓	✓
Incidentlogg med beskrivande texter	-	✓	✓
Stöd för flera omgivningar	✓	-	✓
Nätverkstorlek (Antal enheter i nätverket)	Obegr.	MAX 25st	Obegr.
Egendefinierbara enhetstyper	-	-	✓
Exkluderingsfilter för VPN/SAN/Virtuella Mask.	-	-	✓
Exkluderingsfilter för kapningsdetektering	-	-	✓

LANeye 2.3 Specifikation

Intrångsdetektering	<p>Känsligheten kan ställas in på 3 olika nivåer och omfattar:</p> <ul style="list-style-type: none">- Detekterar nya okända MAC-adresser- Detekterar avvikande IP-adress förfrågningar vid anslutning.- Detekterar avvikande namn och arbetsgrupptillhörighetsförfrågningar.- Detekterar avvikande domäntillhörighetsförfrågningar.- Detekterar oväntat många anslutningsförsök per tidsenhet. <p>Professional Edition har exkluderingsfilter för:</p> <ul style="list-style-type: none">- Kapningsvarningar och misstänkt påloggning.- IP-adress listor för att hantera datorer som flyttas mellan olika nätverk.
Anslutningsblockering	<p>Aktiveras automatiskt när intrång detekteras eller manuell aktivering.</p> <ul style="list-style-type: none">- Blockerar tillgång till nätverket genom nekande av NetBios namn.- Blockerar tillgång till tillåten IP-adress genom försvarande ARP.
Larm	<p>Aktiveras vid intrångsdetektering och/eller anslutningsblockering med:</p> <ul style="list-style-type: none">- Visuellt larm och ljudsignal (eller .wav fil) på lokal dator.- Epost larm. Skickar epostmeddelanden via SMTP med/utan autentisering.
Loggning	<ul style="list-style-type: none">- Incidentlogg där händelser, intrång och blockeringar registreras.- Systemlogg, visar LANeye aktiviteter som driftstart, stopp, larm mm.
Trafikvisning	<ul style="list-style-type: none">- Avsändar och mottagar MAC, IP adresser, protokoll och paketstorlek.- UDP/TCP avsändar och mottagarportnr.- UDP/TCP trafiktyper (http/pop/netbios/ftp/smtp/ssh/telnet/...).- Ethernet trafiktyper (IP/ARP/IPX/IPNG/NOVELL/SNMP/...).
Trafikfilter	<ul style="list-style-type: none">- Multicast paketfilter- Local-administrated paketfilter- Endast skickade paketfilter
Övrig information om nätverksenheter	<ul style="list-style-type: none">- Datum då enheten först påträffades och senast var aktiv.- Nätverksnamn (CIFS/SMB/NETbios/DHCP/DNS)- Fabrikat, Operativsystem, Hur IP adress har tilldelats.- Typ av enhet, Om den har DHCP server, Class ID, CIFS tjänster- MAC-adress, IP adress, Nätmask, Domän, Nätverksgrupp, DNS
Mätare	<ul style="list-style-type: none">- CPU och LAN-kort belastning.
Omgivningshantering	<p>Small Network Edition hantera en omgivning. Professional Edition hantera flera omgivningar. En anges som standard.</p>
Autostart	<p>Kan fås starta och aktiverad när Windows startas.</p>
System	<p>Arbetar i bakgrunden och nås från systemfältet. I systemfältet indikeras aktivitet, antal enheter, antal aktiva enheter och larm.</p>
Hjälpssystem	<ul style="list-style-type: none">- Inbyggd Incidenthjälp kopplad till incidentloggen där händelser som intrång och blockeringar registreras. Hjälpen har beskrivande texter om vad som kan vara naturliga orsaker till händelsen och vad som kan vara intrång.- Inbyggd guide för att träna LANeye på nätverket.- Inbyggd Introduktionsguide och HTML hjälp med snabbdirektlänkar.

LANeye 2.3 Systemkrav

Operativsystem	Windows Vista, Windows XP, Windows 2000, med IE 5 eller högre.
Nätverk	Ethernet
Hårdvara	CPU 500MHz minimum, 1GHz eller snabbare rekommenderas. Grafik SVGA (800x600) 256 färger eller högre. Nätverkskort. (inbyggda nätverkskort, USB, PC-Card och WLAN kort)

LANeye är en produkt från ProPrat, Stockholm Sweden

www.proprat.se | contact@proprat.se

Copyright © ProPrat 2003-2007, All rights reserved.