TUNKEUTUMINEN VAHVUUDEKSI

Case: Kela

Martta Ekosaari

Opinnäytetyö
Maaliskuu 2009

Liiketoiminta ja palvelut

JYVÄSKYLÄN
AMMATTIKORKEAKOULU

JYVÄSKYLÄN
AMMATTIKORKEAKOULU

KUVAILULEHTI
Päivämäärä
9.3.2009

Tekijä(t)	Julkaisun laji	
EKOSAARI, Martta	Opinnäytetyö	
	Sivumäärä 50	Julkaisun kieli Suomi
	Luottamuksellisuus [X] Liite nro 1 on salainen pysyvästi	

Työn nimi
TUNKEUTUMINEN VAHVUUDEKSI
Case:Kela

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Työn ohjaaja(t)
KARHULAHTI, Mika

Toimeksiantaja(t)
Kelan IT-osasto

Tiivistelmä
Opinnäytetyössä tutkittiin tunkeutumisen havaitsemis- (IDS, Intrusion Detection System) ja estojärjestelmiä (IPS, Intrusion Prevention System). Tutkimuskohteena oli Kelalla käytössä oleva Soneran Net Guard -palvelu. Työn toimeksiantajana toimi Kelan IT-osasto.

IDS/IPS-järjestelmät auttavat yrityksiä parantamaan tietojärjestelmiensä turvallisuutta. Näiden järjestelmien ei ole tarkoitus korvata virustorjuntaohjelmia tai palomuuria. IDS:n avulla voidaan havaita mahdollisia tunkeutujia tai muita uhkaavia yrityksiä yrityksen sisä- ja ulkoverkosta. IPS:n avulla voidaan pysäyttää havaittuja hyökkäyksiä.

Opinnäytetyön keskeiseksi näkökulmaksi otettiin yrityksien saama hyöty IDS/IPS-järjestelmistä. Opinnäytetyössä selvitettiin näiden järjestelmien perustoimintatavat. Työssä esiteltiin alan uusimmat teknologiat ja perustoiminnallisuudet. IDS/IPS-järjestelmistä aiheutuvat haasteet ja saavutettavat hyödyt olivat tutkimuksen tarkempina kohteina.

Varsinaisena tutkimuskohteena oli Soneran Net Guard -palvelu. Kyseinen palvelu on Soneran toimittama ja hallinnoima. Tutkimuksen tarkoitus oli selkeyttää palvelun käyttöä Kelalla ja etsiä siihen kehittämisratkaisuja. Opinnäytetyössä selvitettiin palvelun nykytilanne sekä siihen liittyvät sopimusasiat. Palveluun liittyvät ohjelmistot ja raportointimahdollisuudet olivat yksi osa tutkimusta. Työssä tutkittiin Kelan IT-osaston saamia hyötyjä palvelusta. Opinnäytetyön lopussa annettiin Kelan IT-osastolle kehittämisehdotuksia Net Guard -palveluun liittyen. Lisäksi tuloksissa huomioitiin tietohallinnollinen näkökulma sekä uusien IDS/IPS-järjestelmien valinnassa huomioitavia asioita.

Opinnäytetyö on salainen Net Guard -palveluun liittyen sekä Kelaa koskevien tulosten osalta.

Avainsanat (asiasanat)
tietoturva, tietosuoja, pääsynvalvonta, tietoverkot, verkonhallinta

Muut tiedot
Liitteet ovat salaisia pysyvästi. Liite 1, 19 sivua.

JYVÄSKYLÄ UNIVERSITY OF APPLIED SCIENCES

DESCRIPTION
Date 9.3.2009

Author(s)
EKOSAARI, Martta

Type of Publication
Bachelor´s Thesis

Pages
50

Language
Finnish

Confidential
[X] Attachment Nr 1 is permanently confidential

Title
INTRUSION AS ASSET
Case: Kela

Degree Programme
Business Information Systems

Tutor(s)
KARHULAHTI, Mika

Assigned by
Kela, IT-department

Abstract
In the bachelor's thesis intrusion detection (IDS) and prevention (IPS) systems were studied. The research object was Sonera Net Guard service that is used in Kela. The thesis was assigned by the IT Centre of Kela.

IDS/IDP-systems help enterprises improve their data system's security. These systems do not compensate computer virus programs or fire walls. IDS helps find possible intruders or other sinister attempts in or out of the networks. IPS enables stopping the detected attempts.

The focus of the thesis was on the benefit companies gain from IDS/IPS. The bachelor's thesis presents the basic operations of these systems. In addition, the goal was to introduce the latest technologies. The challenges and the gained benefits of the IDS/IPS-systems were also inspected more in detail.

The main objective was the Sonera Net Guard service, which is delivered and administered by Sonera. The purpose of the research was to clarify the use of the service at Kela and to find development solutions for it. The thesis also discusses the present situation and agreemental issues connected with the service as well as the other programs and reporting possibilities of the service. One important study objective was the benefit of the services to Kela's IT Centre. Finally, the thesis gives development proposals connected to the Net Guard service. In addition, the results consider the viewpoint of data administration and issues to be observed when buying new IDS/IPS systems.

The bachelor's thesis is confidential as for Net Guard service and the results for Kela.

Keywords
data security, data privacy, access control, networks, network management

Miscellaneous
Attachments are permanently confidential. Attachment 1, 19 pages.

SISÄLTÖ

KUVIOT

TERMIT

ERP	Emergency Response Plan, tunkeutumistilanteiden toimenpiteet
HIDS	Host-based Detection System, isäntäpohjainen järjestelmä
HTTPS	Hypertext Transfer Protocol Secure, salattu hypertekstin siirtoprotokolla
ICMP	Internet Control Message Protocol, internetin viestin ohjausprotokolla
IDS	Intrusion Detection System, tunkeutumisen havaitseminen
IDP	Intrusion Detection and Prevention, tunkeutumisen havaitseminen ja estäminen
IDPS	Intrusion Detection and Prevention System, tunkeutumisen havaitsemis- ja estojärjestelmä
IPS	Intrusion Prevention System, tunkeutumisen estäminen
LAN	Local Area Network, lähiverkko
MIDS	Manager Intrusion Detection System, tunkeutumisen havaitsemisjärjestelmän hallinta
NBA	Network Behavior Analysis, verkkokäyttäytymisanalyysi
NIDS	Network-Based Intrusion Detection System, verkkopohjainen tunkeutumisen havaitsemisjärjestelmä
NSM	NetScreen-Security Manager, NSM-ohjelman hallintaliittymä
P2P	Peer-to-peer networking, vertaisverkko
SSH	Secure Shell, turvallinen tiedonsiirtomenetelmä

TCP	Transmission Control Protocol, tietoliikenneprotokolla
UDP	User Datagram Protocol, yhteyskäytäntö
VPN	Virtual Private Network, VPN-verkko
WLAN	Wireless Local Area Network, langaton lähiverkko

1 TUNKEUTUJAT TULEVAISUUDEN HAASTEENA

Erilaiset tunkeutumisen havaitsemis- (IDS, Intrusion Detection System) ja estojärjestelmät (IPS, Intrusion Prevention System) ovat tärkeä osa yrityksen tietoturvallisuutta. Niiden merkitys osana yritysten tietoturvaa on kasvanut viime vuosina. Opinnäytetyön myötä lukijat ymmärtävät IDS/IPS-järjestelmien perusidean ja sen, miksi näitä järjestelmiä kannattaa käyttää.

Yritysten tietoturvasta vastaaville henkilöille IDS-järjestelmä antaa mahdollisuuden seurata haitallista liikennettä ja parantaa saatujen tietojen myötä tietoturvajärjestelmiään. IPS-järjestelmä puolestaan voidaan ohjelmoida estämään hyökkäyksiä jopa automaattisesti. Joka päivä saamme lukea jossain päin maailmaa sattuneista tietoturvahyökkäyksistä. Tämän takia jokaisen tietoturvan parissa työskentelevän pitäisi tietää ainakin perusasiat IDS/IPS-järjestelmistä. Nämä järjestelmät ovat kuitenkin haasteellisia yrityksille. Niiden käyttö vaatii jatkuvaa ylläpitämistä ja kehittämistä sekä laajaa ammattitaitoa.

Opinnäytetyö perehtyy Kelalla käytössä olevaan Soneran toimittamaan ja hallinnoimaan Net Guard -palveluun. Palvelu on ollut käytössä Kelalla jo useamman vuoden. Ostetun palvelun hyödyntäminen on kuitenkin jäänyt vuosien varrella vähäiseksi. Tutkielman tarkoitus on selkeyttää Net Guard -palvelun käyttöä Kelalla ja etsiä siihen kehittämisratkaisuja.

Opinnäytetyön tekijän oma ammatillinen osaaminen tulee kasvamaan huomattavasti tämän työn edetessä. Aiheen tutkiminen antaa lisätietoutta verkkojen tietoturvasta sekä itse IDS/IPS-järjestelmistä. Lisäksi opinnäytetyön tekijä perehtyy tarkemmin Kelan verkkoympäristöön ja siinä olemassa oleviin tietoturvaratkaisuihin.

2 TUTKIMUSASETELMA

Luvussa tarkastellaan opinnäytetyön taustateoriaa ja esitellään opinnäytetyön toimeksiantaja. Lisäksi selkeytetään tavoitteita, rajataan tutkimusaluetta sekä esitellään käytetyt tutkimusmenetelmät ja tutkimuskysymykset. Opinnäytetyössä on tarkoitus löytää vastaukset esitettyihin tutkimuskysymyksiin.

2.1 Taustateoria

Opinnäytetyön aihe tulee työelämästä. Kelalla on ollut käytössään IDS/IPS-järjestelmä vuodesta 2003. Kelalle järjestelmä on jäänyt vieraammaksi, koska palvelun hallinnointi on ostettu muualta. Järjestelmän hyödynnettävyyden kannalta on hyvä lisätä osaamista myös Kelan IT-osastolla. Kelalla käytössä oleva IDS/IPS-järjestelmä on hankittu Soneralta Net Guard -palveluna. Palvelu pohjautuu Juniper Networksin tuottamaan ohjelmistoon ja laitteisiin. Palvelua hallinnoi Sonera oman hallintaliittymänsä kautta. Kela voi tarkastella palvelun toimintaa NetScreen-Security Manager (NSM) -järjestelmällä.

Tunkeutumisen havaitsemis- ja estojärjestelmistä on tehty opinnäytetöitä aiemminkin. Aihetta on tutkittu useista eri näkökulmista. On vertailtu eri järjestelmiä, tutkittu käyttöönottoja testi- tai todelliseen ympäristöön ja tehty IDS/IPS-järjestelmän käyttötutkimusta jossakin yrityksessä.

Vuonna 2008 Sironen on tehnyt opinnäytetyön IDPS (Intrusion Detection and Prevention System)-järjestelmän käyttöönotosta. IDPS on lyhempi ilmaisu IDS/IPS-järjestelmästä. Suomessa kyseistä lyhennettä käytetään jonkin verran. Tämä opinnäytetyö pohjautuu samaan järjestelmään kuin Sirosen opinnäytetyö. Sirosen työssä käydään läpi NSM-järjestelmän keskeisimmät osat. Tutkimuksen varsinaisena kohteena oli Juniper Networks IDP -järjestelmän käyttöönotto. Järjestelmän perustana toimi Juniper IDP 200 -sensori (Sironen 2008).

2.2. Toimeksiantajan esittely

Opinnäytetyön toimeksiantajana toimii Kelan IT-osasto (31.12.2008 asti Kelan ATK-keskus). IT-osaston toiminta-ajatuksena on suunnitella, ylläpitää ja kehittää tietojärjestelmiä sekä tuottaa, toimittaa ja hankkia Kelan käyttämät tieto- ja viestintäteknologiajärjestelmät. Sopimuspohjaisesti Kelan IT-osasto toimittaa palveluita myös muiden organisaatioiden käyttöön. (Kelan Intranet 2009.)

IT-osastossa työskentelee 386 henkilöä (tilanne 31.12.2008). Toimintaa on kolmella eri paikkakunnalla: Helsingissä, Jyväskylässä ja Turussa. IT-osasto jakautuu kahteen päälinjaan: IT-käyttöön ja IT-suunnitteluun. (Mt.)

Opinnäytetyön kirjoittaja työskentelee itse Kelan IT-käyttölinjan Verkot ja turva -tiimissä. Kyseisessä tiimissä työskentelee tällä hetkellä seitsemän henkilöä. Opinnäytetyön aihe on osa Verkot ja turva -tiimin työtehtäviä. Tiimin tärkeimmät työtehtävät liittyvät tietoliikenteeseen, -turvaan ja käyttövaltuuksienhallintaan.

2.3 Tavoitteet ja rajaukset

Opinnäytetyössä halutaan saada perustietämys IDS/IPS-järjestelmistä. Toimintaperiaatteet otetaan tarkemman tarkastelun kohteeksi. Näkökohdaksi otetaan myös se, mitä hyötyä yritykset saavat näistä järjestelmistä. Tutkimuksessa perehdytään tarkemmin Kelassa käytössä olevaan Soneran toimittamaan Net Guard -palveluun. Työssä selvitetään ensiksi sopimusasiat ja kartoitetaan nykytilanne. Perusselvitysten jälkeen tutkitaan Net Guard -palvelun toimivuutta ja siihen liittyviä ohjelmistoja. Lopuksi mietitään vaihtoehtoja palvelun parantamiseksi sekä tehdään ehdotuksia jatkotoimenpiteiksi.

Opinnäytetyössä ei tehdä teknisiä muutoksia Net Guard -palveluun. Palvelua hallinnoi Sonera, joka tekee nämä muutokset. Tutkimuksessa ei selvitetä myöskään muiden toimittajien IDS/IPS-järjestelmiä vaan ainoastaan Soneran Net Guard -palvelua.

2.4 Tutkimusmenetelmät

Opinnäytetyössä käytetään kvalitatiivista eli laadullista tutkimusmenetelmää. Tarkempi määrittely on toimintatutkimus. Toimintatutkimus sopii tähän opinnäytetyöhön tutkimusmenetelmäksi. Opinnäytetyöstä löytyy selkeästi kaksi tavoitetta: kehittäminen ja vaikuttaminen. Tutkimuksessa korostuu käytännön ja teorian vuorovaikutuksellinen suhde. (Hirsjärvi, Remes & Sajavaara 2007, 156 - 160; Tutkimustyön perusteet 2008, 5 - 6.)

Tutkimuksen prosesseissa otetaan huomioon omakohtaiset kokemukset ja hyödynnetään teoriatietoa palvelua arvioitaessa. Tyypillistä toimintatutkimuksessa on se, että painotetaan toimintakohtia, jotka huomataan jo alkuvaiheessa epätyydyttäviksi. Työn etenemiseen kuuluvat keskustelut ja kompromissit. (Tutkimustyön perusteet 2008, 5 - 6.)

2.5 Tutkimuskysymykset

Opinnäytetyön tarkoitus on löytää vastaukset alla oleviin tutkimuskysymyksiin.

1. Mitä hyötyä IDS/IPS-järjestelmistä on yrityksille?

2. Mikä on Net Guard -palvelun nykytila Kelalla (sopimusasiat ja tekninen tilanne)?

3. Miten Net Guard -palvelua voitaisiin kehittää Kelalla?

3 TUNKEUTUMISEN HAVAITSEMINEN JA ESTÄMINEN

Luvun alussa tutustutaan lyhyesti tunkeutumisen historiaan. Seuraavaksi selvitetään perusasioita IDS/IPS-järjestelmistä ja tarkastellaan käytettyjä teknologiatyyppejä. Lopuksi perehdytään IDS/IPS-järjestelmien tuomiin haasteisiin ja hyötyihin.

3.1 Historiaa ja taustatietoa

Palomuuri ja virustorjuntaohjelmat eivät ole enää riittävä turva yrityksen tietoliikenteelle. Nykyisin halutaan saada kaikki mahdollinen tieto siitä, mitä yrityksen tietoverkossa liikkuu.

Tähän ilmiöön havahduttiin jo 1990-luvun alkupuolella, jolloin markkinoille tuotiin ensimmäiset varsinaiset IDS-järjestelmät. Näitä järjestelmiä kutsutaan myös verkon hälytysjärjestelmiksi. IDS:n avulla saadaan lisätietoa sisä- ja ulkoverkoissa tapahtuvasta liikenteestä. Tähän kategoriaan kuuluu myös verkon resurssien, sopimattoman toiminnan sekä hyökkäysten tarkkailu. Parhaimmassa tapauksessa voidaan jopa pysäyttää tunkeutuminen ja saada lisätietoja hyökkäyksestä tulevia toimenpiteitä varten. (Thomas 2005, 326.)

Pelkkä IDS/IPS-järjestelmän rakentaminen ei ole kuitenkaan yksistään riittävä toimenpide. Toimiva järjestelmä tarvitsee paljon tukea ympärilleen. Allen (2002, 185) toteaa, että ilman ennakkovalmisteluja on vaikeaa määritellä, onko tunkeilijoita käynyt tai onko niitä vielä järjestelmissä. Tähän liittyy myös vahinkojen laajuuden selvitys sekä se, miten järjestelmä pystytään palauttamaan luotettavaan tilaan.

Tunkeutumisen havaitsemista ja reagointia helpottaa toimintamalli, jollainen jokaisella yrityksellä olisi hyvä olla. Toimintamallin laatiminen aloitetaan luomalla menettelytapoja, joiden tasot seuraavat yrityksen liiketoimintatavoitteita. Yleisempiin menettelytapoihin kuuluvat politiikkamääritykset, toipumis- ja toiminnan jatkuvuussuunnitte-

lu, riskien kartoitus sekä tärkeimpien tietoresurssien tunnistus. Erilaisten vertailuanalyysien perusteella mitataan resurssien tarvetta eriasteiseen suojaamiseen. Toimintamalliin kuuluu oleellisena osana lokien keruu ja muiden tietojen hallinnointi. Lopuksi pitää vielä saada järjestelmät toimimaan ja työntekijät hallinnoimaan niitä. (Allen 2002, 186 - 188.)

3.2 IDS – havaitseminen

Luku tarkentaa tunkeutumisen havaitsemisen toimintamekanismia. Lisäksi perehdytään IDS:n havainnointiluokkiin ja hunajapurkkeihin, joita käytetään houkutuslintuina. Lopuksi mietitään, mitkä ovat toimivan järjestelmän vaatimuksia.

3.2.1 Havaitsemisjärjestelmän toiminta

Thomasin (2005) mukaan tunkeutumisen havaitsemisjärjestelmä muodostuu kolmesta perusedellytyksestä: missä vahditaan, mitä vahditaan ja miten toimitaan. IDS:n sijoituspaikka on siis näistä ensimmäinen edellytys. Toinen edellytys kertoo sen, millaisissa tilanteissa hälytys tehdään tai aloitetaan vaaditut toimenpiteet. Kolmas edellytys antaa ohjeet IDS:n toimintaa varten. (Thomas 2005, 322.)

IDS sijoitetaan verkossa usein moneen eri paikkaan. Tällä toimenpiteellä saadaan organisaation järjestelmät turvallisemmiksi ja suojaus paremmaksi. Tapahtumaluokitus on IDS-järjestelmän perusasia. Kun organisaatio on hankkimassa käyttöönsä IDS:ää, kannattaa huomioida myös seuraavat seikat: tapahtumien korrelointi, keskitetty sensorien hallinta, räätälöitävät tunnusmerkit ja kynnysarvot, väärien hälytysten eliminoiminen, standardeihin perustuva toteutus, tunkeutumisen estotoiminnot, tunnusmerkkien vastaavuuden tarkistus sekä poikkeavuuksien havaitseminen. Vaikka nämä kaikki asiat olisi toteutettu hyvin, pitää muistaa, että IDS ei pysty valvomaan kaikkea mahdollista. (Mts. 326 - 329.)

3.2.2 Havainnointiluokat

Hyökkäyksen havainnointiin voidaan käyttää useita eri tapoja. Ensisijaiset tunkeutumisen havainnointiluokat ovat allekirjoitukseen perustuva, poikkeavuuksiin perustuva

ja tilallinen protokolla-analyysi. IDS/IPS-järjestelmissä käytetään yleensä useampaa tapaa, jolloin hyökkäyksiä voidaan havaita paremmin. (Mell & Scarfone 2007, 2 - 3.)

Allekirjoitukseen perustuva havainnointi

Allekirjoitukseen perustuva havainnointi (Signature-Based Detection) on ensimmäisiä tunnettuja havainnointimetodeja. Menetelmä perustuu tunnettujen tapahtumien etsimiseen. Esimerkiksi jos telnet-yhteydessä havaitaan käyttäjänimenä ”root”, se tunnistetaan välittömästi. Sen käyttäminen on yleensä organisaation tietoturvasäännöstön vastaista toimintaa. Vakoiluohjelmien tunnistaminen on myös tyypillistä tälle havainnointiluokalle. Tämän perusteella sähköpostiviestin aihekentästä voidaan tunnistaa esimerkiksi ”Free Pictures” tai liitetiedoston tiedostonimestä ”freepics.exe”. Edellä mainituiden kaltaisia tunnistamistapoja on useita ja ne vaihtelevat eri järjestelmissä. (Mts. 2 - 4.)

Tämä havainnointitapa ei ole kuitenkaan kovin joustava. Se tunnistaa ainoastaan täsmälleen samanlaiset muodot eli se ei tunnista muunneltuja muotoja. Jos hyökkääjä on laittanut muodokseen ”freepics2.exe”, ja tunnettu muoto on järjestelmässä ”freepics.exe”, hyökkäystä ei saada tunnistettua. Tuntemattomat hyökkäykset jäävät täten huomioimatta allekirjoitukseen perustuvassa havainnoinnissa. (Mts. 2 - 4.)

Voidaan sanoa, että allekirjoitukseen perustuva havainnointi on yksinkertaisin havainnointitapa. Tekniikka perustuu havaittujen pakettien vertailuun hyökkäystietokannan tietojen mukaisesti. Useita monimutkaisempia tapoja, kuten verkkoprotokollia tai ohjelmaprotokollia, ei tämä havainnointitapa ymmärrä. (Mts. 2 - 4.)

Poikkeavuuksiin perustuva havainnointi

Poikkeavuuksiin perustuvassa havainnoinnissa (Anomaly-Based Detection) normaalia toimintaa verrataan poikkeavaan toimintaan. Normaali toiminta on kirjattu profiileihin. Profiileihin on tallennettu tietoa käyttäjistä, työasemista, tietoliikenneyhteyksistä ja sovelluksista. Käyttökelpoinen profiili saadaan tarkkailemalla normaalia toimintaa määrätyn ajan. Ensimmäisen profiilin luominen saattaa kestää useita päiviä, joskus jopa viikkoja. (Mell & Scarfone 2007, 2 - 4 - 2 - 5.)

Poikkeavuuksiin perustuvat profiilit jaetaan kahteen ryhmään: staattiset ja dynaamiset. Staattinen profiili ei muutu sen muodostamisen jälkeen. Jos halutaan muuttaa staattista

profiilia, se pitää luoda kokonaan uudestaan. Dynaaminen profiili ei pysy muuttumattomana. Se muokkaa itseään jatkuvasti saatujen tietojen perusteella. Järjestelmät ja tietoverkot muuttuvat jatkuvasti. Staattinen profiili pitää tämän takia tehdä uudestaan tietyin aikavälein. Jos generointia ei tehdä, staattinen profiili muuttuu pikkuhiljaa epätarkaksi ja virheelliseksi. Dynaamisilla profiileilla on erilaiset ongelmat. Ne ovat alttiita hyökkääjien välttämiskokeiluille. Tämä voi aikaansaada sen, että järjestelmä ei pysty erottamaan hyökkäyksiä normaalista liikenteestä. (Mts. 2 - 5.)

Epänormaali toiminta saattaa tallentua vahingossa profiileihin. Tämä voi johtaa siihen, ettei kaikkia oikeita hyökkäyksiä havaita. Tarkkojen profiilien tekeminen voi olla vaikeaa monimutkaisten järjestelmien takia. Vääriä positiivisia havaintoja tulee myös usein, koska liikenne järjestelmissä muuttuu paljon. (Mts. 2 - 5.)

Tilallinen protokolla-analyysi

Tilallisessa protokolla-analyysissä (Stateful Protocol Analysis) havaittuja tapahtumia verrataan ennalta määriteltyihin profiileihin. Profiilien protokollissa tarkkaillaan tapahtumia tunnistamalla poikkeavuuksia. Tilallinen protokolla-analyysi luottaa järjestelmien toimittamiin yleisiin profiileihin, joissa kerrotaan, miten protokollia pitäisi käyttää ja miten ei. Tilallinen tässä yhteydessä tarkoittaa, että IDS/IPS-järjestelmä pystyy ymmärtämään ja jäljittämään tietoverkkojen tilaa sekä tietoliikenteen ja sovellusten protokollia. (Mts. 2 - 5.)

Käskyjen odottamien järjestysten havaitseminen on mahdollista tilallisessa protokolla-analyysissä. Käytännössä tämä tarkoittaa esimerkiksi toistuvan saman käskyn antamista tai määrätyn käskyn antamista ennen muita odotettuja käskyjä. IDS/IPS-järjestelmät voivat lisäksi kirjata ylös aidot käytetyt istunnot ja nauhoittaa epäilyttävät käytetyt toiminnallisuudet. Tämä auttaa tapahtumien selvitystyössä. (Mts. 2 - 6.)

Tilallisissa protokolla-analyyseissä käytetään protokollamalleja. Mallit perustuvat yleensä protokollastandardeihin, jotka tulevat ohjelmistovalmistajilta tai standardointielimiltä. Standardit eivät aina ole täydellisiä protokollien yksityiskohtien osalta, mikä aiheuttaa puolestaan vaihteluja protokollien toteutuksessa. Useat valmistajat rikkovat standardeja tai lisäävät omia ominaisuuksia niihin. Nämä toimenpiteet saattavat muuttaa standardien määrittelemiä ominaisuuksia. (Mts. 2 - 6.)

3.2.3 Houkutuslinnut

Houkutuslintuja voidaan kutsua tässä asiayhteydessä myös monella muulla nimellä. Englanninkielinen nimitys on yleensä honeypots eli hunajapurkit. Yleensä houkutuslintu näyttää ulospäin tavalliselta järjestelmältä. Siihen ei ole kuitenkaan asennettu mitään normaaleja tuotantokäyttöön liittyviä järjestelmiä. (Thomas 2005, 345.)

Thomas (2005, 345) toteaa kirjassaan, että houkutuslinnut eivät ratkaise yhtään tietoturvaongelmaa. Houkutuslintuja käytetään harhautuksiin, torjuntaan, havaitsemiseen ja tietojen keräämiseen. Ne muistuttavat yleensä jotain oikeata järjestelmää, joka saattaa kiinnostaa hakkereita. Houkutuslintujen tärkeimpiä käyttötarkoituksia ovat:

- hyökkääjien harhauttaminen pois tärkeiden verkkoresurssien luota
- ennakkovaroituksen saaminen uusista hyökkäyksistä
- hyökkääjän toiminnan tarkempi tutkiminen
- tietoturvan tehokkaan suunnittelun varmistaminen ja
- hyökkääjän parempi tunteminen.

Houkutuslintuja käytettäessä pitää muistaa laatia palomuuriin säännöt. Hakkerit tulevat epäluuloisiksi, mikäli tätä ei ole tehty. Asiantuntijoiden mukaan houkutuslintujen pitäisi sallia kaikki liikenne, mutta toiseen suuntaan vain FTP, ICMP ja DNS. Saadut lokit auttavat tulkitsemaan saatuja tuloksia. Houkutuslinnut aiheuttavat kuitenkin joitakin rajoituksia. Ensimmäinen on se, että jos järjestelmään todella tunkeudutaan, niin tämän jälkeen houkutuslintua voidaan käyttää astinlautana verkkoon murtautumiselle. Toiseksi houkutuslinnut tekevät verkosta monimutkaisemman, mikä ei välttämättä ole hyväksi tietoturvan osalta. Lisäksi houkutuslinnut vaativat jatkuvaa ylläpitoa. (Thomas 2005, 348 - 349.)

3.2.4 Oikeanlaisen järjestelmän löytäminen

Markkinoilta löytyy nykyään kymmeniä erilaisia IDS/IPS-järjestelmiä. Suurin osa niistä on kaupallisia ratkaisuja. Markkinoilla on myös avoimeen lähdekoodiin perustuvia järjestelmiä. Tunnetuin niistä on Snort. (Aartolahti 2005.)

Organisaatioilla on siis paljon valinnanvaraa etsiessään itselleen sopivaa IDS-järjestelmää. Ongelmaksi kuitenkin usein muodostuu se, että järjestelmien toimittajat lupaavat valtavan määrän erilaisia ominaisuuksia. Thomasin (2005, 327 - 329) mukaan organisaatioiden kannattaa huomioida seuraavat asiat perinteisen tapahtumalokituksen lisäksi:

- tapahtumien korrelointi
- keskitetty sensorien hallinta
- räätälöitävät tunnusmerkit ja kynnysarvot
- väärien hyökkäysten eliminoiminen
- standardeihin perustuva toteutus
- tunkeutumisen estotoiminnot
- tunnusmerkkien vastaavuuden tarkistus ja
- poikkeavuuksien havaitseminen.

Edellä mainitut ominaisuudet näkyvät itse järjestelmän käytössä. Järjestelmän valinnassa pitäisi huomioida eri osapuolten tarpeita. Hallinnolla ja ylläpitäjillä ei ole samoja vaatimuksia järjestelmälle. Siksi valintaprosessissa olisi hyvä olla edustajia eri tahoilta. Järjestelmän valintaan vaikuttaa myös käytettävissä oleva raha. IDS/IPS-järjestelmissä ostohinta ei kuitenkaan ole ainut aiheutuva kulu. Usein järjestelmistä peritään erilaisia ylläpitomaksuja. Järjestelmän hallinta ja hyödyntäminen vie myös päivittäin työaikaa ylläpitäjiltä.

3.3 IPS – estäminen

Tunkeutumisen estäminen täydentää tunkeutumisen havaitsemista. Tässä luvussa perehdytään IPS:n käyttötarkoitukseen, käytettyihin estomuotoihin sekä toimintaedellytyksiin.

3.3.1 Tarkoitus

Tunkeutumisen estojärjestelmä (Intrusion Prevention System eli IPS) estää hyökkäyksen onnistumisen mahdollisimman varhaisessa vaiheessa. IPS tarvitsee aina kaverikseen toimivan IDS-järjestelmän. IPS on hyödyllinen oikein konfiguroituna, mutta väärin määriteltynä se saattaa aiheuttaa haitallisia seurauksia normaalille verkkoliikenteelle. (Thomas 2005, 337.)

IPS-järjestelmä eroaa IDS-järjestelmästä yhdellä tavalla: IPS:n avulla on mahdollista pysäyttää hyökkäys. Hyökkäykseen pysäyttämiseen on kehitetty erilaisia estomuotoja, joita käsitellään tarkemmin seuraavassa luvussa. Myös käytetty IDS/IPS-teknologiatyyppi vaikuttaa tunkeutumisen estämisen mahdollisuuksiin (ks. IDS/IPS-teknologiat).

3.3.2 Tunkeutumisen estomuodot

IPS-järjestelmät pystyvät pysäyttämään tunkeutumisen. Keinoja estämiseen on useita erilaisia. Mellin ja Scarfonen (2007, 2 - 2 - 2 - 3) mukaan tunkeutumisen estomuodot voidaan jakaa seuraaviin ryhmiin:

- IPS pysäyttää hyökkäyksen.
- IPS muuttaa tietoturvaympäristöä.
- IPS muuttaa hyökkäyksen sisältöä.

Hyökkäyksen pysäyttäminen voidaan tehdä usealla tavalla. Tietoliikenneyhteyden tai käyttäjän istunnon katkaisu on yksi tyypillisimmistä keinoista. Käyttäjätili, IP-osoite tai hyökkäysominaisuus voidaan laittaa sulkulistaan. Sen avulla voidaan estää pääsy

isäntäkoneeseen, palveluun, ohjelmaan tai johonkin muuhun resurssiin. Tietoturvaympäristön muuttaminen tapahtuu häiritsemällä kohdetta. IPS voi muuttaa palomuurin tai reitittimen konfigurointia, jolloin hyökkäys ei enää onnistu. Hyökkäyksen sisällön muuttaminen on mahdollista poistamalla tai korvaamalla joitakin osia hyökkäyksestä. Yksinkertainen esimerkki on saastuneen liitetiedoston poistaminen sähköpostiviestistä. Monimutkaisempi esimerkki on IPS:n muuntautuminen välityspalvelimeksi. Tällöin ns. välityspalvelin hylkää tulleet pyynnöt. Hyökkääjä häiriintyy ja lopettaa hyökkäyksen. (Mell & Scarfone 2007, 2 - 2 - 2 - 3.)

3.3.3 Toimintaedellytykset

IPS:n toiminta on oikein konfiguroituna erittäin tehokas toimenpide hyökkäyksiä vastaan. Tehokkuutensa takia estojärjestelmää ei saa ottaa käyttöön hutiloimalla. Suositeltavaa on, että kaikki muutokset tehdään ensiksi testijärjestelmään ja vasta sen jälkeen ne otetaan tuotantopuolelle käyttöön. Väärillä käskyillä voidaan lamaannuttaa normaalia tuotantojärjestelmää, mikä puolestaan voi aiheuttaa organisaatiolle imagon huonontumista tai rahallisia menetyksiä.

Tunkeutumisen tutkimista ei saa lopettaa siihen, että IPS on estänyt tunkeutumisen. Ylläpitäjän pitää selvittää, onko hyökkäys ehtinyt tekemään tuhojaan ennen IPS:n toimimista. Hyökkäyksen vakavuudesta riippuen voidaan joutua palauttamaan vanhoja varmistuksia tai jopa sulkemaan hyökkäyksen kohteena ollut palvelu. Lisäksi pitää löytää reitti, mitä kautta hyökkäys on tapahtunut. Tämän jälkeen voidaan tehdä tarvittavia toimenpiteitä, kuten päivittää käytetyn palvelun käyttöjärjestelmä tai itse sovellus. Organisaation tietoturvapolitiikan pitäisi määrittää ohjeet ylläpitäjille erilaisia tilanteita varten. (Thomas 2005.)

3.4 IDS/IPS-teknologiat

Mellin ja Scarfonen (2007, ES - 1) mukaan IDS/IPS-teknologiat luokitellaan tapahtumatyypeittäin neljään eri luokkaan. Vielä pari vuotta sitten luokittelu oli erilainen. Kaksi luokitteluluokkaa ei ole kuitenkaan muuttunut näinä vuosina perusasioiltaan. Verkkopohjaiset (Network-Based) ja isäntäpohjaiset (Host-Based) ovat perinteisim-

mät ja samalla tunnetuimmat tavat. Kaksi muuta teknologiaa ovat langaton (Wireless) ja verkkokäyttäytymisanalyysi (Network Behavior Analysis). (Mts. ES - 1.)

3.4.1 Verkkopohjainen

Network-Based eli verkkopohjainen teknologia on tunnetuin ja tällä hetkellä myös käytetyin muoto tunkeutumisen havaitsemis- ja estojärjestelmissä. Verkkopohjaista järjestelmää kutsutaan usein lyhenteellä NIDS (Network-Based Intrusion Detection System). (Mell & Scarfone 2007, 4 - 1 - 4 - 15.)

Verkkopohjaisen järjestelmän ideana on valvoa ja analysoida verkkojen, verkkoliikennöinnin ja ohjelmien protokollatoimintoja verkkosegmenteissä ja -laitteissa. Tavoitteena on löytää epäilyttäviä tapahtumia, joita voidaan käsitellä määritellyllä tavalla. Verkkopohjaiset järjestelmät sijaitsevat yleensä verkkojen rajapinnoissa. Tavallisimpia paikkoja ovat palomuurin, reitittimen, langattoman verkon tai VPN-palvelimen läheisyys. (Mts. 4 - 1 - 4 - 15.)

Tämä teknologia perustuu sensoreiden toimintaan. Käytettävät komponentit ovat samankaltaisia kuin muissa teknologiatyypeissä. Näitä komponentteja ovat sensoreiden lisäksi hallintapalvelimet, konsolit ja tietokantapalvelimet. Verkkopohjaisia järjestelmiä myydään myös ilman laitteita. Tämä pitää huomioida hankittaessa IDS-järjestelmää. (Mts. 4 - 3 - 4 - 4.)

Mellin ja Scarfonen (2007, 4 - 4) teoksessa verkkopohjaiset järjestelmät jaetaan kahteen ryhmään sensorien sijainnin perusteella: aktiivisiin (Inline) ja passiivisiin (Passive) tiloihin. Aktiivisessa tilassa verkkoliikenne kulkee sensorin läpi. Toimintatapa on samantyylinen kuin palomuurissa. Tämä mahdollistaa myös hyökkäysten estämisen reaaliajassa. Tyypillinen sijoituspaikka on kahden verkkolaitteen välissä. Passiivisessa tilassa monitorit ottavat kopion verkkoliikenteestä. Alkuperäinen verkkoliikenne ei siis kulje sensorin läpi. Tämä tapa ei aiheuta hidastelua verkkoliikenteelle. Passiiviset sensorit voivat estää TCP-liikennettä, mutta usein toimenpide on liian hidas johtuen sensorin sijainnista. UDP- ja ICMP-istuntoja eivät voi passiiviset sensorit pysäyttää. Sekä passiiviset että aktiiviset sensorit voivat kuitenkin konfiguroida uudelleen tietoliikenteen turvallisuuteen liittyviä laitteita. (Mts. 4 - 4 - 4 - 6.)

Verkkopohjaisten IDS/IPS-järjestelmien tiedonhankintakyky on rajallinen. Ne pystyvät kuitenkin saamaan tietoja työasemista, käyttöjärjestelmistä, sovelluksista tai tietoverkkojen erityisominaisuuksista. Havaituista tapahtumista voidaan kerätä tietoa lokeihin. Niihin tallentuu esimerkiksi aikaleima, tapahtuman tyyppi, lähde- ja kohdeosoite sekä toimitetun tiedon määrä. (Mts. 4 - 7 - 4 - 8.)

Jokaisessa teknologiassa on huonot puolensa. Verkkopohjaiset järjestelmät eivät pysty havaitsemaan hyökkäyksiä salatusta liikenteestä (esim. VPN, HTTPS, SSH). Sensorit pitäisi sijoittaa tämän takia niin, että ne pystyisivät tarkastelemaan liikennettä sekä ennen että jälkeen salauksen. Toinen merkittävä asia on se, että verkkopohjaiset järjestelmät eivät pysty tekemään täydellistä analyysia suuren kuorman alla. Jotta tärkeät tiedot saataisiin hyvin analysoitua, näissä järjestelmissä kannattaa osa liikenteestä jättää tarkistamatta. (Mts. 4 - 11 - 4 - 12.)

3.4.2 Isäntäpohjainen

Host-Based- eli isäntäpohjaisia järjestelmiä kutsutaan usein lyhenteellä HIDS. Perustoimintapa on aivan erilainen kuin verkkopohjaisissa järjestelmissä. Isäntäpohjaisissa järjestelmissä verkkoliikenteen tarkkailu tapahtuu verkkoon kytkettyjen työasemien kautta. Tarkkailun kohteena on vain siihen työasemaan tuleva ja lähtevä verkkoliikenne. (Aartolahti 2005, 25.)

Tyypillisiä käyttökohteita ovat langallinen ja langaton verkkoliikenne, järjestelmälokit, prosessit, tiedostoihin pääsy ja niiden muokkaaminen sekä järjestelmien ja ohjelmien konfiguratiomuutokset. Toiminta perustuu agentteihin, joiden avulla valvontaohjelmat seuraavat yksittäisen koneen tapahtumia. Agenttien tiedot on kuvattu suojatussa serverissä, pöytäkoneessa, kannettavassa tai ohjelmapalvelussa. (Mell & Scarfone 2007, 7 - 1.)

Isäntäpohjaisten IDS/IPS-järjestelmien verkkoarkkitehtuuri on yleensä melko yksinkertainen. Havainnointiohjelmat toimivat usein työasemissa. Tämän takia komponentit keskustelevat olemassa olevien verkojen välityksellä hallintoverkon sijasta. Järjestelmien suunnittelussa pitääkin huomioida tarkkaan agenttien sijainnit, tarve aktiiviseen analysointiin, käyttöönoton hinta, ylläpito, järjestelmän hallinta, käyttöjärjestel-

mien ja ohjelmien tuki agenteille sekä verkon kyky välittää valvontaohjelmien liikennettä. (Mts. 7 - 2 - 7 - 8.)

3.4.3 Langaton

Langaton (Wireless) teknologia perustuu langattoman verkkoliikenteen tarkkailuun ja sen protokollien epäilyttävien tapahtumien tunnistamiseen (Mell & Scarfone 2007, 5-1). Langattomassa teknologiassa käytetään samoja komponentteja kuin verkkopohjaisessa. Käytettyjä komponentteja ovat konsolit, tietokantapalvelimet, hallintapalvelimet ja sensorit. Tämä teknologia eroaa kuitenkin suuresti verkkopohjaisesta teknologiasta. Langaton teknologia pystyy valvomaan vain yhtä kanavaa kerrallaan. Tämän takia langattomissa järjestelmissä sensorit vaihtavat valvottavaa kanavaa usein, jolloin jokaista kanavaa valvotaan muutaman kerran sekunnissa. (Mts. 5 - 1 - 5 - 4.)

Sensoreita on olemassa monentyyppisiä. Passiivisia (Dedicated) sensoreita on kiinteitä ja mobiililaitteille tarkoitettuja. Mobiililaite-sensori ei kuljeta verkkoliikennettä lähettäjältä vastaanottajalle. Muut sensori-tyypit ovat paketoituja (Bundled): Access Point eli AP ja langaton kytkin (wireless switch). Passiiviset sensorit havaitsevat paremmin hyökkäyksiä kuin paketoidut sensorit. Tämä johtuu siitä, että niiden ei tarvitse käyttää aikaa liikenteen välittämiseen. Passiivisten sensoreiden huonoja puolia ovat korkeammat perustamis-, asennus- ja ylläpitokustannukset. Hintaero johtuu siitä, että paketoidut sensorit voidaan asentaa olemassa oleviin laitteisiin. Passiiviset sensorit puolestaan tarvitsevat toimiakseen muita laitteita tai ohjelmia. (Mts. 5 - 4 - 5 - 5.)

Langattoman järjestelmän komponentit ovat yleensä yhteydessä toisiinsa. Langallisen ja langattoman välimaasto pitää olla tarkasti valvottu, joten usein käytetään hallintaverkkoa tai standardoitua verkkoa järjestelmän komponenttina. Langattoman sensorin sijoituspaikan löytäminen on vaikeampaa kuin muissa teknologioissa. Sijoituspaikan valinnassa pitää huomioida fyysinen turvallisuus, sensoreiden toiminta-alue, langattoman verkon saatavuus, hinta ja paketoidut sensorivaihtoehdot. (Mts. 5 - 5 – 5 - 6.)

Tyypillistä on, että langaton teknologia pystyy keräämään tietoa tarkkailemalla langattomia laitteita ja verkkoja sekä tehdä kattavia lokitiedostoja. Langattomat IDS/IPS-järjestelmät voivat havaita hyökkäyksiä, vääriä konfiguratioita ja sääntöjen loukkaa-

misia. Hyökkääjän sijainti voidaan saada selville kolmiopaikannuksen avulla. (Mts. 5 - 12.)

Tunkeutumisen estäminen on mahdollista myös langattomien sensoreiden avulla. Ne voivat pysäyttää hyökkäyksiä ja estää uuden istunnon muodostamista. Ylläpitäjät voivat konfiguroida langattomia sensoreita ja asettaa niihin haluttuja hälytyksiä. Langattomilla sensoreilla voi olla hieman erityylisiä toimintatapoja, joten niiden valinnassa pitää olla tarkkana, jotta halutut toimenpiteet olisivat mahdollisia. (Mts. 5 - 11.)

3.4.4 Verkkokäyttäytymisanalyysi

Verkkokäyttäytymisanalyysissä (Network Behavior Analysis, NBA) tarkkaillaan verkkoliikennettä ja sen tilastoja. Tarkoituksena on havaita epänormaalia liikennettä. NBA-järjestelmissä käytetään sensoreita ja konsoleita. Osa NBA-sensoreista on samankaltaisia kuin verkkopohjaiset sensorit. Ne tarkastelevat paketteja seuratessaan aktiivista verkkoa yhdessä tai useammassa verkon segmentissä. Muun tyyppiset NBA-sensorit eivät pysty valvomaan verkkoa suoraan. (Mts. 6 - 1.)

Mellin ja Scarfonen (2007, 6 - 2) mukaan useimmat NBA-sensorit toimivat vain passiivisessa tilassa. Ne pitäisi sijoittaa niin, että ne voivat valvoa tärkeimpiä verkon osa-alueita. Aktiivisia sensoreita käytetään yleensä harkitusti verkkojen reuna-alueilla. Tällöin ne pystyvät paremmin rajoittamaan hyökkäyksiä.

NBA-järjestelmät tarjoavat laajan valikoiman tietoturvaan liittyviä asioita. Ne pystyvät keräämään yksityiskohtaista tietoa työasemista sekä valvomaan tietoliikennettä ja siinä tapahtuneita muutoksia. Tämä teknologia pystyy havaitsemaan useita erilaisia haitallisia tapahtumia, kuten palvelunestohyökkäyksiä, skannauksia, matoja, odottamattomia ohjelmamuutoksia ja tietoturvasääntöjen vastaisia rikkomuksia. NBA-järjestelmien hyvä puoli on se, että ne pystyvät tutkimaan lyhyessä ajassa suuren määrän verkkoliikennettä. Monet NBA-sensorit voivat koota uudelleen tapahtumaketjun alkuperäisen uhan selvittämiseksi. (Mts. 6 - 4.)

NBA-tuotteille on ominaista, että ne päivittyvät automaattisesti. Ylläpitäjien pitää päivittää vain palomuurin sääntölistaa. Jotkut NBA-tuotteet tarjoavat allekirjoitukseen perustuvia sääntöjä. Niistä saattaa olla apua käytettäessä aktiivisia sensoreita. NBA-

teknologioista löytyy merkittäviä rajoituksia. Hyökkäyksen havaitsemisessa saattaa esiintyä viivettä järjestelmän käyttämien tietolähteiden takia. Toinen merkittävä rajoitus liittyy siihen, että yksittäinen sensori pystyy analysoimaan useaa verkkoa, mutta valvomaan vain muutamaa verkkoa samanaikaisesti. (Mts. 6 - 8.)

3.5 IDS/IPS-järjestelmien haasteet

IDS/IPS-järjestelmä ei voi olla koskaan täydellinen. Osa saaduista havainnoista on vääriä positiivisia ja osa vääriä negatiivisia. Nämä molemmat ryhmät aiheuttavat ylimääräistä päänvaivaa järjestelmän ylläpitäjille. Väärä positiivinen tarkoittaa, että IDS/IPS-järjestelmä tulkitsee oikean toiminnan tunkeutumiseksi. Väärä negatiivinen puolestaan ilmaisee sen, että oikea tunkeutuminen on jäänyt havaitsematta. Tyypillisin virhe järjestelmän ylläpitäjillä onkin, että järjestelmää säädetään väärin, jolloin edellä mainittuja tapahtumia tulee liikaa. Vääriltä havainnoilta ei voi kuitenkaan koskaan täysin välttyä. (Mell & Scarfone 2007, 2 - 8.)

Tunkeutumisen havaitsemis- ja estojärjestelmän hallinta on yksi suurimmista järjestelmän toimivuuteen vaikuttavista tekijöistä. Prosessi alkaa oikeastaan jo järjestelmän suunnittelu- ja hankintavaiheesta. Väärällä valinnalla ei saavuteta haluttua hyötyä yritykselle. Rahallinen panostus varsinkin isoissa organisaatioissa on usein suuri. Oletetaan, että organisaatiolle on valittu oikeanlainen IDS/IPS-järjestelmä. Käyttöönottokin on sujunut hyvin. Tämän jälkeen kuitenkin järjestelmä jätetään huomioimatta. Tällöin järjestelmästä ei ole hyötyä, vaan pikkuhiljaa se menettää täysin merkityksensä. Järjestelmää pitää siis jatkuvasti säätää, päivittää sekä tulkita saatuja raportteja.

Päivittäinen käyttö onkin yksi IDS/IPS-järjestelmän tärkeimmistä asioista parhaan mahdollisen hyödyn aikaansaamiseksi. Olisi siis hyvä tarkastella joka päivä saatuja tapahtumia, analysoida mielenkiintoiset tapahtumat sekä tehdä raportteja. Mellin ja Scarfonen (2007, 9 - 10) mukaan päivittäisen käytön suunnittelussa pitäisi huomioida seuraavat asiat:

- Miten tapahtumat ja hälytykset näytetään käyttäjille, mitä ominaisuuksia näytetään pika-analyysissä, kuinka käyttäjät voivat räätälöidä näkymiä ja filttereitä?

- Kuinka näytetään saadut tiedot käyttäjille ja ylläpitäjille?

- Kuinka järjestelmä ilmoittaa hälytyksistä, järjestelmän vioista ja muista toiminnallisista ongelmista?

- Kuinka paljon näytetään lisätietoa tapahtumista?

- Kuinka monta käyttöliittymää/ohjelmaa tarvitaan päivittäisiä tehtäviä varten?

- Kuinka monta samanaikaista käyttöliittymää on tuettu?

IDS/IPS-järjestelmien ylläpitäjiltä vaaditaan laajaa tietotaitoa useilta eri osa-alueilta. Ylläpitäjän pitää ymmärtää organisaation kokonaiskuva tietoverkoista, tietoturvasta, järjestelmän eri osa-alueista sekä tietysti hallita itse IDS/IPS-järjestelmä. Lisäksi tarvitaan tietoa organisaation tietoturvasäännöistä ja -politiikasta. Järjestelmän ylläpitäjän pitää siis oikeastaan tietää kaikesta mahdollisesta mikä liittyy jollain tavalla tietojärjestelmiin. Mell ja Scarfone (2007, 3 - 9) ovat maininneet teoksessaan seuraavat asiat: tietoliikenneprotokollat, erilaiset ohjelmat ja käyttöjärjestelmät.

Aiemmin tässä työssä kerrottiin neljästä eri teknologiatyypistä: Network-Based, Host-Based, Wireless ja Network Behavior Analysis. Jokainen näistä tarjoaa hieman erityylistä tietoa. Jokaisella teknologiatyypillä on hyvät ja huonot puolensa. Suositeltavaa onkin, että organisaatiot käyttäisivät eri teknologioihin perustuvia IDS/IPS-järjestelmiä samanaikaisesti. Myös eri valmistajien tuotteet saattavat täydentää toinen toisiaan. Usean eri järjestelmän yhtäaikainen käyttö vaatii kuitenkin todella laajaa tietämystä. (Mell & Scarfone 2007, 8 - 1.)

3.6 IDS/IPS-järjestelmien hyödyt

IDS-järjestelmän tavoitteena on löytää tapahtumia, jotka ovat tietoturvapolitiikan vastaisia tai muuten loukkaavat organisaation toimintaa. Saaduilla tuloksilla voidaan siis löytää haittaohjelmia, internetin kautta tulleita luvattomia yrityksiä sekä havaita organisaation omia käyttäjiä jotka haluavat aiheuttaa tuhoa (Mell & Scarfone 2007, 2 - 1).

Järjestelmän avulla on mahdollista tuottaa tietoa havaituista tapahtumista, ilmoittaa ylläpitäjälle tärkeistä tapahtumista ja tuottaa raportteja (Mts. 2 - 8). Täydellisen hyödyn saamiseksi yrityksellä pitää olla turvapolitiikka, jossa käsitellään tunkeutumisen havaitsemiseen ja reagointiin liittyvät toimenpiteet. Tietoturvapolitiikan ymmärrystä ja osaamista pitää olla sekä järjestelmän käyttäjillä että hallinnosta vastaavilla henkilöillä. Turvapolitiikan avulla voidaan tositilanteissa toimia organisaation turvapolitiikan mukaisesti. Näin aikaa jää paremmin fyysisen tason toimenpiteisiin, kun päälinjaus on selvillä. (Mts. 2 - 8.)

Allen (2002) kertoo, kuinka tärkeää on määritellä turvapolitiikkaan liittyvä valmistautuminen sekä toteuttaa valmistautumistoimenpiteet. Turvapolitiikassa määritellään säännöt, jotka opastavat organisaatiota hallitsemaan ja turvaamaan tieto- ja tietojärjestelmäresurssejaan turvallisuustavoitteidensa mukaisesti. Menettelytapaohjeilla jokaisen työntekijän pitäisi pystyä toimimaan turvapolitiikan mukaisesti. Yritys hyötyy näistä ohjeista, koska työntekijät tietävät tällöin paremmin oikeat toimintatavat ja velvollisuudet käyttäytyä tietoresursseja kohtaan. (Allen 2002, 187 - 189.)

IDS:n tarkoituksena on löytää tunkeutumiset tai niiden yritykset. IPS puolestaan estää tunkeutujaa. Jos järjestelmä on oikein konfiguroitu, suurin osa vakavista yrityksistä saadaan havainnoitua ja/tai estettyä. Oikein toimiessaan IDS/IPS-järjestelmä ilmoittaa saaduista löydöistä myös järjestelmien ylläpitäjille. Hälytysmuotona voi olla prioriteetin mukaan esimerkiksi sähköposti tai tekstiviesti. Kaikista saaduista lokitapahtumista ei hälytystä lähetetä. Tarkkailemalla näitä lokitapahtumia saatetaan löytää myös pienempiä tunkeutumisen yrityksiä, jotka on kuitenkin hyvä estää.

Tunkeutumisen havaitseminen ja estäminen on IDS/IPS-järjestelmien päätarkoitus. Useat yritykset ovat kuitenkin löytäneet järjestelmille myös muuta hyötykäyttöä. Tähän luokkaan kuuluu samaistuminen tietoturvasääntöjen ongelmiin. Jotkut IDS/IPS-

järjestelmät voivat siis huomata esimerkiksi väärin konfiguroidut palomuurisäännökset. Olemassa olevien uhkien dokumentointi on toinen näistä muista käyttötavoista. Tätä voi hyödyntää siten, että tulkitsemalla saadut tapahtumat voidaan paremmin huomioida organisaation tärkeitä resursseja. Saatu tieto auttaa lisäksi uhkien hallinnoimisessa, mikä puolestaan tarkoittaa, että organisaation julkisivu pysyy puhtaampana. Yksittäisten tietoturvarikkomusten estäminen on myös yksi hyvä tapa. Järjestelmän avulla voidaan saada havaintoja esimerkiksi siitä, että yksittäisen käyttäjän teot eivät ole täysin laillisia. Jo tässä vaiheessa voidaan varoittaa tai estää käyttäjää toimimasta niin. (Mell & Scarfone 2007, 2 - 1 - 2 - 2.)

Otettaessa käyttöön IDS/IPS-järjestelmää organisaatiot voivat opettaa järjestelmää halutunlaiseksi. Näissä toimenpiteissä kuitenkin pitää olla varovainen, jotta haluttu hyöty ei aiheuta päinvastaista tulosta. Kynnysarvojen avulla määritellään raja-arvoja, jolloin kynnysarvojen ulkopuolella olevista asioista saadaan raportteja. Näin tapahtuu, jos käyttäjä esimerkiksi laittaa väärin salasanan kymmenen kertaa kolmen minuutin sisällä. Tällöin voidaan saada kiinni henkilöt, jotka yrittävät käyttää jonkun toisen tunnusta hyväkseen. (Mts. 3 - 3.)

Musta lista (black list) on luettelo erilaisista tapahtumista, jotka ovat havaittu haitallisiksi. Mustasta listasta käytetään usein nimeä hot list eli kuuma lista. IDS/IPS-järjestelmissä mustaa listaa käytetään mahdollisten tunkeutujien havaitsemisessa ja estämisessä. Valkoiselle listalle (white list) laitetaan tapahtumia, jotka eivät aiheuta haittaa järjestelmille ja ovat muutenkin tunnettuja. Hälytysasetusten avulla saadaan organisaatiolle tiedot hälytyksistä oikeaan aikaan ja oikeaan paikaan. Jotkut IDS/IPS-järjestelmät sallivat myös koodin muokkauksen, jolloin organisaatio voi räätälöidä järjestelmän asetuksia paremmin omia tarpeitaan vastaaviksi. (Mts. 3 - 3.)

4 SONERAN NET GUARD -PALVELU

Palvelu esitetään liitteessä 1.

4.1 Yleisesittely

4.1.1 Toimintaperiaate

4.1.2 Tekninen tausta ja havaitsemisen lähtökohdat

4.1.3 Palvelurakenne ja raportointi

4.2 Lähtökohdat ja nykytilanne Kelalla

4.2.1 Sopimus ja laskutusperiaatteet

4.2.2 Palvelukuvaus ja -ajat

4.2.3 Esitutkimus ja verkkosuunnitelma

4.2.4 Sensorit

4.2.5 Tunkeutumistilanteiden toimenpiteet

4.2.6 Raportointi SurfManager:lla

4.2.7 Valvonta

4.3 Netscreen-Security Manager

4.4 Palvelun kehittäminen Kelalla

5 TUTKIMUKSEN TOTEUTUS

Tutkimuksen toteutus esitetään liitteessä 1.

6 JOHTOPÄÄTÖKSET

Johtopäätökset esitetään liitteessä 1.

6.1 Tulosten yleistä tarkastelua ja arviointia

6.2 Pohdinta

LÄHTEET

Allen, J. 2002. CERT Verkkotietoturvan hallinta. Helsinki: Edita.

Aartolahti, A. 2005. IDS-järjestelmän käyttöönotto opetusympäristössä. Opinnäytetyö. Jyväskylän ammattikorkeakoulu, tekniikka ja liikenne, Informaatioteknologian instituutti.

Emergency Response Plan – Tunkeutumistilanteiden toimenpiteet. 2003. Sonera.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2007. Tutki ja kirjoita. 13 p., osin uud. laitos. Helsinki: Tammi.

Kelan Intranet-sivut. 2009. Viitattu 8.1.2009.

Knowledge Base: Juniper Networks. 2008. Viitattu 15.1.2009. Http://kb.juniper.net/KB10528.

Mell, P & Scarfone, K. 2007. Guide to Intrusion Detection and Prevantion Systems (IDPS). Tulostettu 8.12.2008 http://www.csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

NetScreen-Security Manager Online Help. 2008. Juniper Networs.

Sironen, T. 2008. IDPS-järjestelmän käyttöönotto yrityksen tuotantoverkossa. Opinnäytetyö. Jyväskylän ammattikorkeakoulu, Tekniikka ja liikenne, Informaatioteknologian instituutti.

Sonera IDS -sopimus. 2003. Helsinki.

Sonera lasku 9/2008.

Sonera Net Guard -palvelukuvaus. 2007. Helsinki.

Sonera Net Guard -esitys. 2008.

Sonera SurfManager -käyttöohje. 2008. Ohje, 136 - 140.

Soneralta uusi tunkeutumisen havainnointi- ja estopalvelu yrityksille. 2004. Tulostettu 28.12.2008. Lehdistötiedote. Http://www.teliasonera.fi/press, lehdistötiedotteet.

Thomas, T. 2005. Verkkojen tietoturva perusteet. Helsinki: Edita.

Tutkimustyön perusteet. 2008. Jyväskylän ammattikorkeakoulu.