EESTI ETTEVÕTLUSKÕRGKOOL MAINOR
Veebidisaini ja digitaalgraafika õppekava

Mari-Liis Truija

SOLARWINDS TURVASÜDMUSE HALDUR

Iseseisev töö

Juhendaja: Hillar Põldmaa

Tallinn 2022

1. SISSETUNGIMISE TUVASTAMISE SÜSTEEM (IDS)

Sissetungituvastussüsteem (IDS) jälgib võrgu- ja süsteemiliiklust ükskõik mis kahtlase tegevuse suhtes. Ohtude avastades saadab tarkvara (näiteks SolarWinds) nendest hoiatavaid teavitusi. Tõhus lahendus peaks suutma avastada ohud enne, kui need süsteemi jõuavad sattuda. Sissetungituvastussüsteemi tarkvara on tavaliselt ainult üks osa turvalahenduste infosüsteemide kaitsmiseks. Lihtne tulemüür loob küll aluse võrgu tuvalisusele, kuid paljud arenenud ohud võivad sellest mööda hiilida. Täisväärtuslik turvalahendus sisaldab sissetungivastase kaitse osana ka autoriseerimise ja autentimise juurdepääsu kontrolli meetmeid. IDS lisab täiendava kaitseliini, muutes ründaja jaoks juurdepääsu organisatsiooni võrgule raskemaks.

2. IDS TÜÜBID

Sissetungituvastussüsteemi on kahte tüüpi: hostipõhine sissetungituvastussüsteem (HIDS), mis uurib sündmusi isikliku arvuti võrku ühendatud arvutis või võrgupõhine sissetungituvastussüsteem (NIDS), mis uurib võrguliiklust. Hostipõhine IDS (HIDS) on juurutatud konkreetses lõpp-punktis ja loodud kaitsma seda sisemiste ja välimiste ohtude eest. Saab jälgida võrguliiklust arvutite vahel, jälgida jooksvaid protsesse ja kontrollida süsteemi logisid. Võrgupõhine IDS (NIDS) on loodud kogu kaitstud võrgu jälgimiseks. See jälgib kogu võrgu liikuvust ja teeb otsusteid pakettide metaandmete ja sisu põhjal. Pakub rohkem võimalusi laialt levinud ohtude avastamiseks. Küll aga puudub NIDSil nähtavus nende kaitstud lõpp-punktide sisemustele.

3. HIDS VS NIDS

Ettevõtte seisukohalt peaks valima nii HIDSi kui NIDSi. NIDS annab palju rohkem jälgimisvõimet, võimaldades küberrünnakud reaalajas kinni pidada. HIDS jällegi suudab tuvastada kui midagi on valesti alles siis, kui seadet või faili on juba muudetud. Nende kahe süsteemi kombineerimine moodustab kokku väga hea pahavara ennetava lahenduse.

4. SOLARWINDS SEM

SolarWinds Secutiry Event Manager (SEM) ehk SolarWinds turvasündmuse haldur sisaldab andmete kontrollimise tööriistu, et tsentraliseerida võrgus töötava tarkvara loodud logide või sündmuste salvestamine ja tõlgendamine. See kogub erinevatest allikatest logisid, kontrollib logid läbi ja paneb need loetavasse vormingusse. SolarWinds SEM on mugav lahendus ettevõttele erienevate võimalike ohtude uurimiseks ja ennetamiseks ning audititeks valmistumiseks.

SolarWinds SEM kasutab ohtude tuvastamisel väga head lähenemist. Võrgu sissetungimise tuvastamise süsteemi logisid kogudes kogub SEM teavet rünnakutüüpide ja -summade kohta. Seejärel integreeritakse see teave teiste infrastruktuuri logidega, luues ohtude avastamiseks suure andmevõrgu. Need andmed optimeerivad pidevalt IDS-i turvasüsteeme ja -protsesse või teavitavad võrgu kaitsmiseks paremini varustatud tõhusamate protseduuride loomisest. SEM-iga saate tuvastada võrgus probleemsed seadmed, kasutada andmeid sidusrühmade jaoks riskianalüüsi aruannete koostamiseks ja tuvastada kõrgelt arenenud ohud enne, kui need teie süsteemi jõuavad.

SEM kasutab natiivset tehnoloogiat, et säästa teie aega, mis muidu kuluks rutiinsete ülesannete täitmisele. See teeb seda jälgides ja hoiatades teid mis tahes kahtlastest sündmustest või tegevustest ning tegutsedes automaatselt, kui tuvastatakse konkreetsed sündmused. See juurutab võrguandureid, mis aitavad tuvastada sissetungi, viib läbi andmete analüüsi, tuvastab tarbitavad teenused ja automatiseerib varade leidmise.

SolarWinds SEM on tehtud ajapikku väga kasutajasõbralikuks. Selle kasutajaliides on lihtne ja funktsionaalsused on kergesti kättesaadavad ülemise juurdepääsuriba tõttu. Kõik vahekaardid on kiiresti navigeeritavad ning andmete esitamine toimub graafikute kaudu ja andmed on kergesti loetavad. Visuaalselt on dashboard ehk armatuurlaud puhas, selge, piisavalt värviline, et tähelepanu juhtida tähtsatele kontadele, ilma segadust tekitavate vidinateta ja dünaamiline.

SolarWinds pakub SEM-i 30-päevast tasuta prooviversioon See on saadaval Windowsi, Unixi, Linuxi ja Mac OS-i kasutajate jaoks.

Siia on lisatud ka näide SolarWinds SEM dashboardist. Visuaalselt näeb puhtam ja loetavam välja võrreldes teiste sissetungituvastussüsteemi tarkvaradega (Zeek, Kismet, Security Onion jpt.).