Bruker dokumentasjon
Webtrafikk sikkerhet

Universitet i Stavanger

Universitetet
i Stavanger

Innhold

Universitetet
i Stavanger

UiS Webtrafikk sikkerhet

Bakgrunn

UiS har i henhold til gjennomførte Risiko og Sårbarhetsanalyser (ROS), anskaffet et verktøy for å øke sikkerheten for UiS brukerne når de bruker internettet, dette er Trend Micro InterScan Web Security Virtual Appliance (IWSVA).

Formålet med å dette verktøyet er å forhindre at ondsinnet kode fra internettet infiserer UiS arbeidsstasjoner via webtrafikk, det vil si, internet browsing (http) eller filoverføringer (ftp).

Dette kan for eksempel skje ved at en bruker leser en webside som er infisert med spyware, skjult redirigering til en annen webside, skjulte Java script, cross-site scripting og annen avansert ondsinnet kode. Majoriteten av malware (ondsinnet kode) hosts er i dag legitime websider som har blitt kompromittert.

Hvorfor introduserer UiS Webtrafikk sikkerhet?

I dag er trusselbildet for hackerangrep via internettet karakterisert av organisert kriminalitet, som har utnyttet utviklingen av internettet til å lage en kraftig underjordisk økonomi. To hovedutfordringer preger dagens sikkerhetsløsninger:

- En dramatisk endring i trusselbildet har produsert mye mer kompliserte trusler.
- En eksplosjon i antall trusler har gjort at tradisjonell beskyttelse mot ondsinnet kode som er basert på nedlastning av signatur filer, slik som anti-virus, ofte er for sein til å fange opp ny og sofistikert ondsinnet kode og krever stadige hyppige oppdateringer.

Det kreves derfor en løsning som raskt kan stoppe ny ondsinnet kode og som er i stand til å oppdage oppførsel som isolert sett ikke ville kunne identifiseres som angrep, men som kan gjenkjennes ved å korrelere dette med annen informasjon.

Hvordan virker Webtrafikk sikkerhet?

Webtrafikk sikkerhet virker ved at trafikk fra og til en bruker ikke sendes direkte til internettet, men går via UiS Internett gateway servere (Trend IWSVA servere) som sjekker websiden brukeren går mot for ondsinnet kode, og stopper ondsinnet kode før denne når brukerens arbeidsstasjon.

Det er kun ondsinnet kode som vil bli stoppet, UiS internett gateway servere vil ikke filtrere hvilken trafikk som tillates.

Hva må brukeren gjøre for å bruke Webtrafikk sikkerhet?

Trafikken fra brukerne som skal til internettet vil automatisk bli sendt via UiS Internett gateway slik at brukeren ikke behøver gjøre noen endringer på sin arbeidsstasjon for å få bedre beskyttelse mot ondsinnet kode fra websider.

Hvordan virker Trend IWSVA?

Trend Micro InterScan Web Security Virtual Appliance (IWSVA) er basert på bruk av både lokale sikkerhets komponenter installert på serverne, og distribuerte (in-the-cloud) sikkerhets komponenter, disse kalles Trend Micro Smart Protection Network.

A. Distribuerte sikkerhetskomponenter- Trend Micro Smart Protection Network

Trend Micro Smart Protection Network består av følgende hovedkomponenter:

1. Web Reputation Service
2. Email Reputation
3. File Reputation
4. Correlation with Behaviour Analysis
5. Smart Feedback
6. Threat Intelligence

1. Web Reputation Service

Dette er en cloud basert tjeneste som bruker domain reputation (rykte) databaser for å angi sikkerhetsrisiko for web domain (for eksempel uis.no), websider og objekter på web sider basert på alder, hvor ofte et domain er blitt flyttet mellom Internet Service Providers (ISPer), og indikasjoner om mistenkelige aktiviteter oppdaget gjennom typisk malware (ondsinnet kode) mønster.

Web Reputation (web omdømme) tjenesten blir kontinuerlig oppdatert, og innhold fra web sider som har et dårlig rykte blir stoppet før det når brukerens nettverk eller arbeidsstasjon.

Retursvaret fra web serveren blir videre skannet i følge http og ftp skann regler på den lokale Trend IWSVA serveren før det sendes til brukeren. Lokal IWSVA skanning og filter tjenester inkluderer URL Filtering, Antivirus og Spyware,

Trend IWSVA serveren bruker et Web Reputation Cache for å redusere behovet for å sende ut forespørsler til den cloud baserte tjenesten, noe som reduserer forsinkelser og forkorter tiden det tar for å gjøre http oppslag.

Dersom det ikke finnes noen gradering for det forespurte materialet, og Tend IWSVA serveren får tilbakemeldig om ”ukjent”, aktiveres følgende to prosesser:

Trends cloud baserte Web Reputation tjeneste starter en automatisk prosess for å tråle gjennom websiden som er forespurt og analysere innholdet. Trends Web Reputation Database blir oppdatert med resultatet slik at den neste forespørsel for det samme web innholdet blir besvart av Web Reputation tjenesten.

Trend IWSVA serveren skanner det ukjente web innholdet med sin lokale skanner tjeneste.

Skann resultatet blir sent tilbake til den cloud baserte Web Reputation tjenesten gjennom Page Analysis og Feedback loop.

2. File Reputation
Cyber kriminelle flytter ofte individuelle filer med ondsinnet innhold fra en web side til en annen for å unngå oppdagelse, noe som gjør at sjekking av en fils omdømme eller rykte er et viktig sikkerhetsmoment. File Reputation teknologi sjekker ryktet for en fil mot Trends File Reputation cloud baserte tjeneste før en tillater en bruker å laste ned filen. Dette gjelder også filer som er sendt som vedlegg i email.

3. Correlation and Behavior Analysis
Korrelasjons og mønster (Correlation and Behavior) analyse er en Trend Micro bakgrunns tjeneste som korrelerer (sammenholder) aktiviter fra flere Smart Protection nettverks komponenter for å se om et mønster som indikerer ondsinnet hensikt kan finnes.

4. Smart Feedback
Trend Micro produkter installert hos kunder sender informasjon om nye trusler som er blitt identifisert tilbake til Trends Smart Protection nettverk.

B. Lokale sikkerhets komponenter:

De lokale sikkerhetskomponentene brukes av Trend IWSVA Scan Engine.

1. URL Filtrering
   URL Filtrering er basert på klassifisering av URLs. Trend IWSVAs URL Filtering tjeneste korrelerer (sammenligner) sine Sikkerhetskategori graderinger med Trends Web Reputation Service database. Dette betyr at klassifiseringen av URLs kontinuerlig blir oppdatert med siste informasjon.
2. AntiVirus
3. Spyware
4. Heuristics
5. True File Type
6. Applet & ActiveX
7. andre

Protokoller og trafikkflyt

UiS Web innholdskontroll servere Trend IWSVA vil beskytte følgende trafikk som sendes mot internettet:

- **HTTP**

Tabell 1 Protokoller og trafikkflyt

Web aksess-metode	**Beskrivelse av aksessmetode**	**Hva gjør Trend IWSVA for denne aksessmetoden?**
http	Ukryptert forbindelse til en webside, data sendes i klartekst mellom klienten og websiden. Når en skriver for eksempel www.google.no, vil dette resultere i en http forbindelse til http://www.google.no/ Det er websiden (URL) som definerer hvilken aksessmetode som brukes, enten ukryptert via http eller autentisert og kryptert vha. https.	1) http forespørsel skannes enten mot lokal cache eller mot Trend Smart Protection Network. 2)Avhengig av resultatet vil forespørselen sendes videre til web serveren på internettet. 3) Returtrafikken fra webserveren skannes av Trend IWSVA serveren for ondsinnet kode før den sendes videre til klienten.

Hva er ondsinnet kode og hvilken trafikk vil bli stoppet?

Nedenfor listes noen typer ondsinnet kode:

Phishing (Fisking)

Dersom Trend IWSVA gjenkjenner en webside som en Phishing URL, vil brukerens trafikk stoppes før den når websiden.
En Phishing webside forsøker å lure brukeren til oppgi personlig eller finansiell informasjon som vil brukes til å stjele brukerens identitet.

Definisjon:
Phishing: A fraudulent collection of confidential information. This can be done by offering an email message or Web site that poses as a communication from a legitimate business, which requests information for the purpose of identity theft.

Spyware (Spionprogram)

Dersom Trend IWSVA serverne gjenkjenner at en webside inneholder et program som i det skjulte samler inn konfidensiell informasjon om brukeren vil brukerens trafikk til dette programmet stoppes.

Definisjon:
Spyware: A hidden but legal program that secretly collects confidential information. Spyware monitors a user's computing habits and personal information, and then sends this information to third parties without the user's approval.

Virus accomplice (Virus forbindelse)

Dersom Trend IWSVA serverne gjenkjenner ondsinnet oppførsel i en brukers utgående HTTP forespørsel så er dette tegn på at brukerens arbeidsstasjon er infisert med spyware eller trojaner, og trafikken stoppes.

Definisjon:
Virus accomplice: An outbound HTTP request due to known behavior of malicious code—the malicious code could either send the information out or download further components from a certain URL. These are the symptoms of a spyware or Trojan infection.

Disease Vector(Ondsinnet webside)

Dersom Trend IWSVA serverne gjenkjenner at en webside kun er satt opp for å spre ondsinnet kode stoppes brukerens trafikk mot denne websiden.

Definisjon:
Disease vector: A Web site that exists only for a malicious purpose

Hvilke meldinger kan en bruker få?

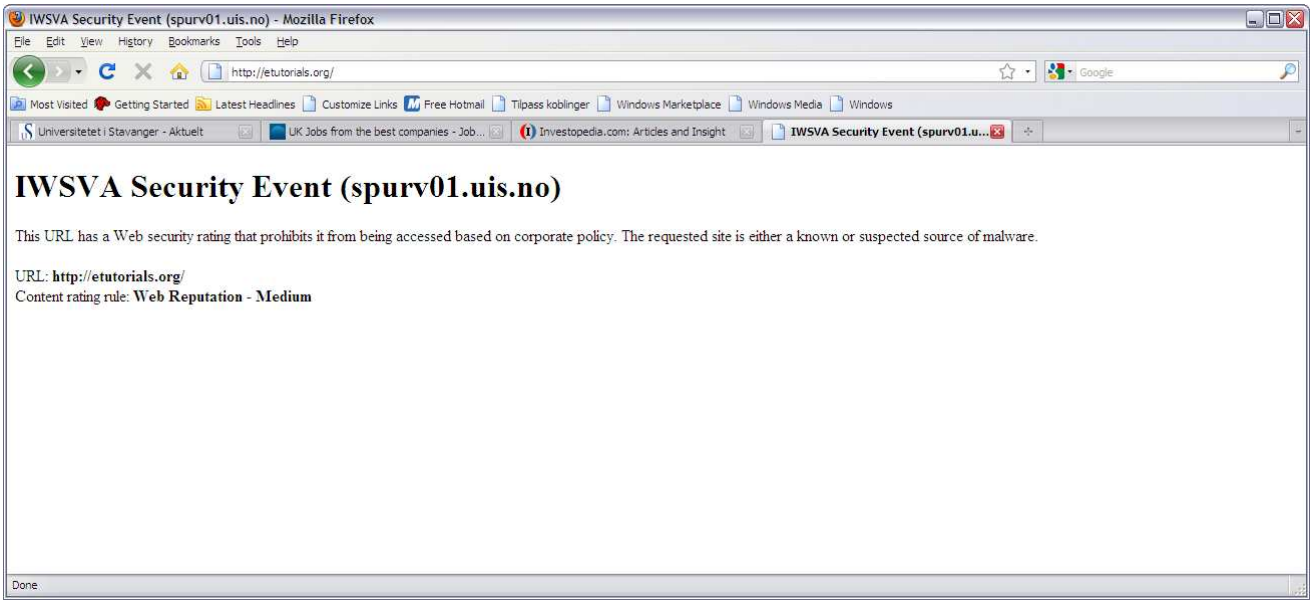
Brukeren vil få en melding i sin web browser dersom Trend IWSVA serverne har oppdaget ondsinnet kode i en webside.

Meldingen som gis vil variere avhengig av hvilken type ondsinnet kode som er oppdaget.

Noen ganger vil det kun være deler av en webside som inneholder ondsinnet kode, da er det bare trafikk mot denne delen av websiden som vil stanses.

Eksempel: URL blokkeres basert på dårlig rykte- Web Reputation

Dersom en bruker forsøker å gå til en webside som med høy sannsynlighet eller påviselig er kompromittert med ondsinnet kode vil en melding som vist nedenfor vises og brukerens sesjon vil stoppes før den når websiden slik at infeksjon unngås.



Vil brukeren se andre endringer?

Nedlasting av filer

Når en bruker laster ned en fil fra internettet vil Trend IWSVA serverne skanne filen for virus eller annen ondsinnet kode. Det betyr at brukeren noen ganger kan oppleve en liten pause i nedlastningen mens skanning foregår, deretter lastes filen ned som normalt.