Openbare Samenvatting

CyberDEW
Een “Distributed Early Warning” Systeem ten behoeve van Cyber Security

Cyber Security

Onderzoeksthema Malware

Projectnummer SBIR13C043

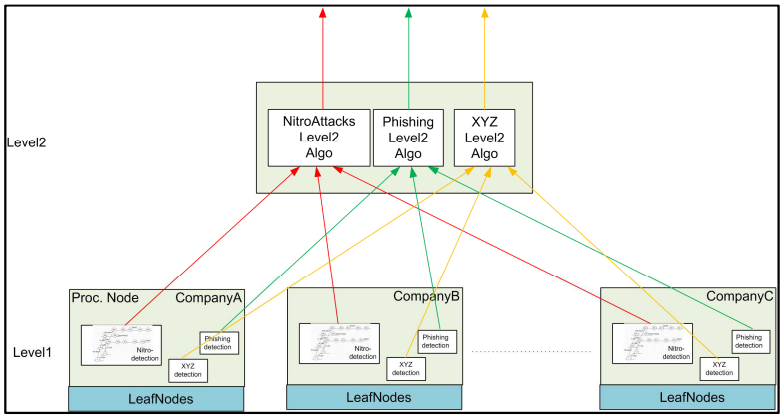
Datum:
27 februari 2015

THALES

Project titel
CyberDEW

Bedrijf
Thales Cybersecurity NL, in samenwerking met Thales Research & Technology Nederland, Hogeschool Rotterdam en het Wetenschappelijk Onderzoeks- en Documentatie Centrum van het Ministerie van Veiligheid en Justitie.

Het probleem
Cybersecurity incidenten worden gedetecteerd door het combineren van informatie, afkomstig van een veelheid van sensoren. Detectie kan lokaal plaatsvinden, het nadeel is dat er, zeker voor geavanceerde aanvallen, te weinig informatie beschikbaar is. Detectie kan ook centraal plaatsvinden, het nadeel hiervan kan zijn dat er teveel informatie aangeboden wordt en waardoor de relevante signalen niet gevonden worden. De uitdaging is de juiste balans te vinden.



Oplossing
De juiste balans wordt in de CyberDEW oplossing geboden door het lokaal interpreteren van zogenaamde “zwakke signalen”. Zwakke signalen hoeven op zichzelf niets te betekenen maar kunnen, op basis van kennis van een aanval en gecombineerd met andere zwakke signalen, aanleiding geven tot het vermoeden, een waarschijnlijkheid, dat een aanval voorbereid wordt of plaatsvindt. Deze vermoedens worden volgens een hiërarchie gedeeld met het naast hogere niveau(s) en op basis van domeinkennis en andere informatie (bijv. actueel dreigingsbeeld) verrijkt. Het onderliggende processing framework maakt het gemakkelijk informatieverwerkingseenheden toe te voegen, te koppelen en van nieuwe algorithmen te voorzien. Uitwisseling van informatie tussen nodes wordt beveiligd door de toepassing van een veilig (secure) data distributie systeem.

Voorbeeld, vermoedens van een Nitro-aanval
Als voorbeeld worden de Nitro-aanvallen genomen. De “Nitro-attacks” is een aanvalscampagne uitgevoerd midden 2011 met als doel het stelen van Intellectueel Eigendom, wereldwijd. Deze aanvallen worden goed begrepen en volgen een mechanisme dat nog steeds actueel is. De met de aanval gepaard gaande “zwakke signalen” (verkregen op netwerk- en applicatie niveau) worden met een speciaal algorithme gecombineerd tot een waarschijnlijkheid dat het om een “Nitro-attack”. Deze waarschijnlijkheid wordt gevisualiseerd zodat een Security Officer snel inzicht heeft en verdere stappen kan nemen.

Status

De in dit SBIR-project ontwikkelde technologie biedt goede mogelijkheden tot aanvulling van Intrusion Detectie functionaliteit. Genoemde technologie wordt verder ontwikkeld en zal dienst gaan doen in volgende generaties van Security Incident & Event Management (SIEM) – systemen.

Over Thales Nederland

Thales Nederland BV is de Nederlandse vestiging van de internationale Thales Group. In Nederland werken ongeveer 2000 medewerkers in de vestigingen in Hengelo, Huizen, Delft en Eindhoven. Thales Nederland is gespecialiseerd in de ontwikkeling, productie en integratie van complexe hightech systemen voor de defensie, transport en veiligheidsindustrie zoals radar, mission management systems, OV chipkaart, communicatie systemen en cybersecurity monitoring.

Met security monitoring services voorziet Thales in de behoefte van nieuwe en grootschalige oplossingen in cybersecurity. Met deze services wordt bijgedragen aan continuïteit, bestendigheid en weerbaarheid van multinationals, centrale overheden en vitale infrastructuren. De afgewogen balans van preventieve en correctieve maatregelen zorgt voor optimale security. Het op de locatie Huizen, door Thales gebouwde en geëxploiteerde, monitoring center biedt elk van haar klanten het verlangde niveau van momentaan inzicht in de staat van haar cybersecurity.

Contact gegevens

Thales Cybersecurity Nederland
Postbus 88
1270 AB Huizen
Nederland

www.thalesgroup.com/nl