Memo

INTERnet ABUSE Detectie Systeem (INTERADS)

Datum
23 november 2015

Classificatie
Publiek

Auteur
SIDN Labs

Blad
1/2

Contact
T 026 352 55 00
support@sidn.nl
www.sidn.nl

Bezoekadres
Meander 501
6825 MD Arnhem

Postadres
Postbus 5022
6802 EA Arnhem

Naam onderzoek/applicatie	INTERnet Abuse Detectie Systeem (INTERADS)
Ingangsdatum Policy	23 november 2015
Doel van de applicatie of het onderzoek	Het doel van INTERADS is om de data uit het ENTRADA-platform te analyseren en te classificeren op basis van (nog te bedenken) algoritmes. Een voorbeeld hiervan is het detecteren van botnets, phishing, IP-spoofing of andere vormen van internet-abuse. Daarnaast is het doel van het project te onderzoeken welke andere afnemers naast de Abuse Information Exchange een toegevoegde waarde zien in de ENTRADA-data en daardoor met het systeem willen koppelen. Dit alles moet ervoor zorgen dat het internet nog veiliger, beter en betrouwbaarder wordt.
Persoonsgegevens	Om het bovenstaande doel te kunnen bereiken, hebben we de volgende gegevens nodig uit het ENTRADA-platform: • IP-adressen • DNS-querydata Tijden en frequentie bezochte domeinen
Grondslag	Gerechtvaardigd belang.
Filters	De gepubliceerde documenten worden geanonimiseerd.
Retentie	We bewaren de gegevens gedurende de loop van het onderzoek. Na afronding van het onderzoek verwijderen we de gegevens van de lokale schijven en de Windesheim Community.

Toegang

We slaan de gegevens op op de servers van Windesheim en de laptops van de projectleden. De fysieke toegang tot de servers van Windesheim is hiertoe beperkt. Alleen de systeembeheerders van Windesheim kunnen fysiek bij de servers. Toegang tot de data online is via gebruikersnaam, wachtwoord en toegekende rechten afgeschermd.

De personen die toegang hebben tot de gegevens zijn:

- Manager SIDN Labs
- Medewerker SIDN Labs die studenten begeleidt
- Multidisciplinair team van studenten van Hogeschool Windesheim

Publicatie/delen

We delen de gegevens met een partij buiten SIDN; deze partij bestaat uit een multidisciplinair team (studenten) van Hogeschool Windesheim, dat dit project uitvoert.

SIDN en Hogeschool Windesheim sluiten een overeenkomst met een uitwerking van de gegevensverstrekking en bijbehorende voorwaarden.

Type

R&D Onderzoek

Andere beveiligingsmaatregelen

Laptops projectleden:

- Alle projectleden loggen in met minimaal een gebruikersnaam en wachtwoord.
- Alle projectleden gebruiken een vorm van encryptie om de ontvangen gegevens op te slaan (bijvoorbeeld VeraCrypt, Bitlocker fulldisk of folder encryption).

Windesheim Community:

- De Windesheim Community maakt gebruik van SSL (communities.windesheim.nl).
- Privé community, alleen beschikbaar voor projectleden, Manager SIDN Labs en de SIDN Labs medewerker die de projectleden begeleidt..