Passive DNS Data Sharing an SIE Europe

Überblick:

Der Security Information Exchange of Europe (SIE Europe.NET) ist ein Managed Network, durch das Data Sharing Teilnehmer Netzwerktelemetrie gemeinsam mit vertrauenswürdigen Datenanalysten in beinahe Echtzeit austauschen können. Diese vertrauenswürdigen Analysten setzen sich u. a. aus Vertretern von akademischen Einrichtungen, aber auch aus weiteren Data Sharing Teilnehmern zusammen. Das Ziel der SIE Europe ist es, den Blick auf europäische Daten zu verbessern und dadurch das Internet sicherer zu machen. Dieses Dokument bezieht sich hauptsächlich auf passive DNS. Aber in Zukunft sollen auch Network Telescope Output, Spam Trap Output sowie Honeypot Output als Datenquellen unterstützt werden.

Details:

Data Sharing Teilnehmer, die einen oder mehrere Recursive Domain Name System (RDNS) Server betreiben, installieren SIE Europe's passive DNS Sensor auf Open-Source-Software-Basis an oder in der Nähe eines solchen Servers. Dies erfolgt z.B. indem ein passiver Netzwerk Tap vor den Name Server geschaltet wird oder durch das Konfigurieren eines „Span Ports" an den vorgelagerten Ethernet Switch des Name Servers. Weitere Möglichkeiten sind die direkte Installation des passive DNS Sensors auf dem Name Server selbst oder die Nutzung des frei zugänglichen dnstap Protokolls, um einen nahegelegenen Telemetry Collection Server zu erreichen.

Der Output des Software Sensors ist ein Datenstrom von DNS-Transaktionen, bestehend aus der Anfrage, der Rückmeldung und verschiedenen Messdaten, wie etwa die Gesamtdauer der Transaktion. Dabei ist es unser striktes Konzept, dass der Output keine personenbezogenen Daten enthält. Der Sensor überwacht lediglich den Datenverkehr ins Internet falls das RDNS keine Antwort liefert (Cache Miss Traffic). Auf den nachgelagerten Datenverkehr, der die IP-Adresse des Endnutzers preisgeben würde und häufige Muster wiederkehrender Aufrufe ermitteln könnte, hat der Sensor jedoch keinen Zugriff.

Der Sensor-Output kann entweder mittels des trampoline Protokolls direkt an SIE Europe übermittelt werden oder vorerst im Security Operations Center (SOC) des Data Sharing Teilnehmers gesammelt werden. Dort kann er, neben der Weiterleitung an SIE Europe zum Zweck umfangreichen Data Sharings, gespeichert und analysiert werden. SIE Europe empfiehlt allen Data Sharing Teilnehmern diesen Datenverkehr zu sammeln, zu speichern und zu analysieren, um die Kenntnisse über das eigene Netzwerk zu verbessern. Damit die externe Analyse für andere Data Sharing Teilnehmer erleichtert wird, verlangen die Richtlinien der SIE Europe, dass einmal gesammelte Daten zusätzlich an SIE Europe weitergeleitet werden.

Status:

Weltweit haben mehr als einhundert Unternehmen, Dienstleister, akademische - und Forschungseinrichtungen diese passive DNS Sensoren installiert und teilen ihren DNS-Transaktionsdatenfluss in annähernd Echtzeit. Jeder Data Sharing Teilnehmer erhält Zugriff auf geteilte Daten anderer Mitglieder, die sowohl in nahezu Echtzeit als auch in aufgezeichneter Form zur Verfügung stehen. Dies führt dazu, dass alle teilnehmenden Netzwerke besser überwacht werden können und gleichzeitig in der Lage sind, sowohl legitimen als auch auffälligen Datenverkehr innerhalb der europäischen Internetwirtschaft besser zu beobachten.

Nächste Schritte:

Als erstes muss zwischen SIE Europe und einem neuen Data Sharing Teilnehmer ein Data Participant Abkommen unterzeichnet werden, dass die Rechte und Pflichten jeder Vertragspartei darlegt. Es entfallen keine Gebühren für Aufnahme und Mitgliedschaft.

Danach folgen technische Maßnahmen, wie Beratung bezüglich der Topologie und Methodik, Lieferung und Installation der Sensorsoftware, Austausch von Authentifizierungskeys, initiale Inbetriebnahme sowie das Einstellen von Rahmenbedingungen und Methoden zur fortlaufenden Überwachung und Störungsbehebung.

Topologie: