

PRESSEINFORMATION

Cybersicherheit durch Visual Analytics optimieren

PRESSEINFORMATION9. Dezember 2021 || Seite 1 | 4

Sechs Stunden ohne Facebook, Instagram und Co.: Für die US-amerikanische Facebook Inc. bedeutete dies Milliardenverluste. Doch wie kommt es zu solchen Problemen und wie lassen sie sich möglichst schnell erkennen? Mit diesem Themenkomplex beschäftigt sich das Fraunhofer IGD bereits seit mehreren Jahren und verfolgt mit dem Forschungszentrum ATHENE das Ziel, Netzwerkdaten verständlicher zu machen. Somit werden mehr Menschen befähigt, einzuschätzen, was im eigenen Netzwerk passiert. Aktuelle und künftige Möglichkeiten zur visuellen Analyse sollen die Arbeit der Sicherheitsexperten vereinfachen.

»Die Masse an angezeigten Warnungen, die für mehr Cybersicherheit sorgen sollen, ist in Unternehmensnetzwerken kaum überschaubar«, sagt Prof. Dr. Jörn Kohlhammer, ATHENE-Wissenschaftler beim Fraunhofer-Institut für Graphische Datenverarbeitung IGD. Das Problem dabei sei, dass ein Großteil der Nachrichten aus Warnungen bestünde, die durch ungefährliche Besonderheiten im Netzwerkverkehr zu Stande kämen. »Dies kann dazu führen, dass die Meldungen, bei denen tatsächlich Handlungsbedarf besteht, in diesen False Positives untergehen. Die Unsicherheit darüber, welche Warnungen als erstes zu behandeln sind, ist dabei ein drängendes Problem.«

Ein weiteres Beispiel für unübersichtliche Datenmassen ist das Border Gateway Protocol (BGP). Dieses ist das Routingprotokoll, das autonome Systeme verbindet und den grenzübergreifenden Datenverkehr des Internets ermöglicht. Wie wichtig dies ist, zeigte der Ausfall von Facebook-Services Anfang Oktober. Aufgrund einer Wartung auf Seiten von Facebook kam es zu einer Unterbrechung der Verbindungen der DNS-Server zum Rechenzentrum. Diese hielten daraufhin BGP-Ankündigungen zurück, da eine gestörte Netzverbindung vorzuliegen schien. Die Server waren länger nicht erreichbar. Mit einer besseren Übersicht der BGP-Ankündigungen wäre dies zu verhindern gewesen.

PRESSEINFORMATION

Die Unübersichtlichkeit der Datenmengen macht es vor allem kleineren Unternehmen schwer, einen Überblick über ihre Cybersicherheit zu gewährleisten. Die Lösung ist aus Sicht des Fraunhofer IGD die zielgerichtete Visualisierung von sicherheitsrelevanten Daten und Informationen, denn: Je einfacher Netzwerkdaten verständlich gemacht werden, desto mehr Menschen können einschätzen, was im eigenen Netzwerk passiert.

Im Rahmen des Nationalen Forschungszentrums für angewandte Cybersicherheit ATHENE beschäftigt sich das Fraunhofer IGD mit Lösungen zur Visualisierung von Cybersicherheitsdaten. Hersteller von Cybersicherheitssoftware können von dieser Expertise profitieren: Softwarelösungen, die schon heute über gute Funktionalitäten verfügen, können durch eine verbesserte Visualisierung Effektivität und Nutzerzufriedenheit steigern. Ziel ist die Schaffung von Benutzeroberflächen, die bei der Verwendung sehr großer Datenmengen unterstützen und speziell auf die Aufgaben von Netzwerkadministratoren und Sicherheitsexperten ausgerichtet sind.

Visual Analytics sorgt für Überblick

Schon heute bietet das Fraunhofer IGD zahlreiche Lösungen im Bereich der Visual Analytics. So können Cybersicherheitsexperten visuell und interaktiv Warnungen zu verschiedenen Gruppen zuordnen, ohne lange Listen durchzugehen und jede Warnung einzeln beurteilen zu müssen. Stattdessen werden ähnlichen Warnungen als benachbarte Blasen visualisiert, die interaktiv gemeinsam in verschiedene Gruppen eingeteilt werden können.

Das Werkzeug NetCapVis visualisiert Netzwerkdaten sortiert nach Kriterien wie IP-Adressen oder Datenformat. Auf einem Zeitstrahl ist ersichtlich, zu welchem Zeitpunkt welche Datenpakete in das Netzwerk gelangen oder das Netzwerk verlassen. Auf diese Weise ist ein schneller Überblick gegeben, der gleichzeitig eine gezielte Reaktion auf unbekannte Datenbewegungen ermöglicht.

»Die Leitfrage unserer Forschung lautet: Wie kann man Interfaces so vereinfachen und verbessern, dass immer weniger Vorwissen nötig ist, um die Sicherheit des eigenen Netzwerkes zu überwachen«, so Prof. Dr. Kohlhammer. In Zeiten von Digitalisierung und zunehmenden Angriffen auf Unternehmen und öf-

FRAUNHOFER-INSTITUT FÜR GRAPHISCHE DATENVERARBEITUNG IGD

PRESSEINFORMATION

fentliche Einrichtungen sei dies wichtiger denn je. »Das große Ziel ist die bestmögliche Unterstützung von Netzwerkadministratoren und Sicherheitsexperten durch die Visualisierung von Cybersicherheitsdaten.«

PRESSEINFORMATION

9. Dezember 2021 || Seite 3 | 4

Weiterführende Informationen:

Zur Visual Analytics Forschung des Fraunhofer IGD:

www.igd.fraunhofer.de/kompetenzen/technologien/visual-analytics

Zum Nationalen Forschungszentrum für Angewandte Cybersicherheit ATHENE:

www.athene-center.de/

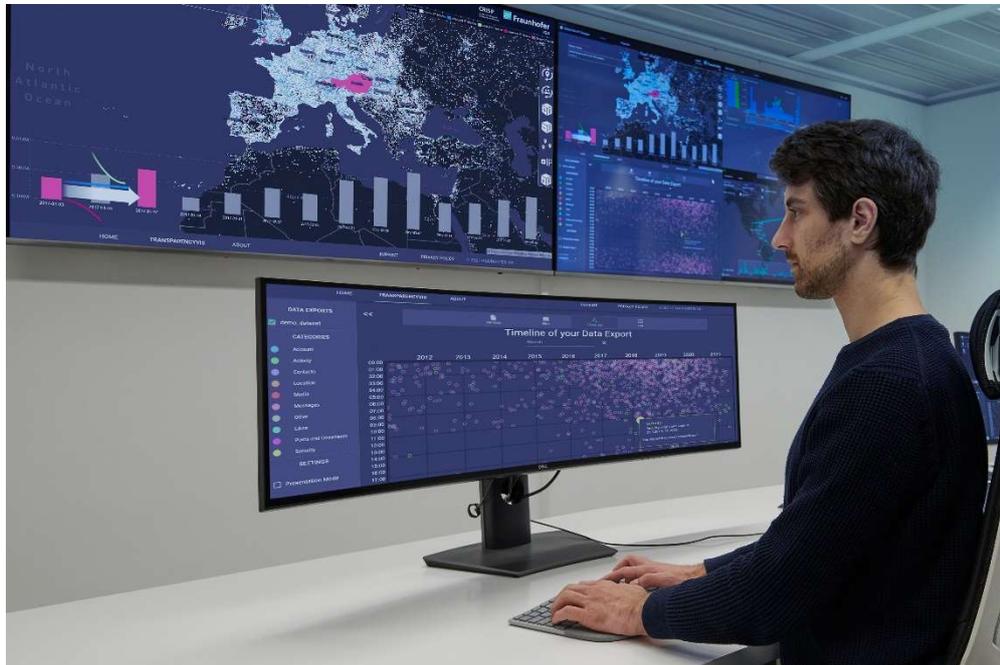


Bild (M): Visualisierungen sicherheitsrelevanter Daten unterstützen Sicherheitsexperten bei der Überwachung des eigenen Netzwerkes (© Fraunhofer IGD).

PRESSEINFORMATION

Über das Fraunhofer IGD

Das 1987 gegründete Fraunhofer-Institut für Graphische Datenverarbeitung IGD ist die international führende Einrichtung für angewandte Forschung im Visual Computing, der bild- und modellbasierten Informatik. Wir verwandeln Informationen in Bilder und Bilder in Informationen. Stichworte sind Mensch-Maschine-Interaktion, Virtual und Augmented Reality, künstliche Intelligenz, interaktive Simulation, Modellbildung sowie 3D-Druck und 3D-Scanning. Rund 180 Forscherinnen und Forscher entwickeln an den drei Standorten Darmstadt, Rostock und Kiel neue technologische Anwendungslösungen und Prototypen für die Industrie 4.0, das digitale Gesundheitswesen und die »Smart City«. Durch die Zusammenarbeit mit den Schwester-Instituten in Graz und Singapur entfalten diese auch internationale Relevanz. Mit einem jährlichen Forschungsvolumen von 21 Mio. Euro unterstützen wir durch angewandte Forschung die strategische Entwicklung von Industrie und Wirtschaft.

PRESSEINFORMATION9. Dezember 2021 || Seite 4 | 4
