

EINHALTUNG DER DSGVO IN DER FORENSIK

PROBLEM:

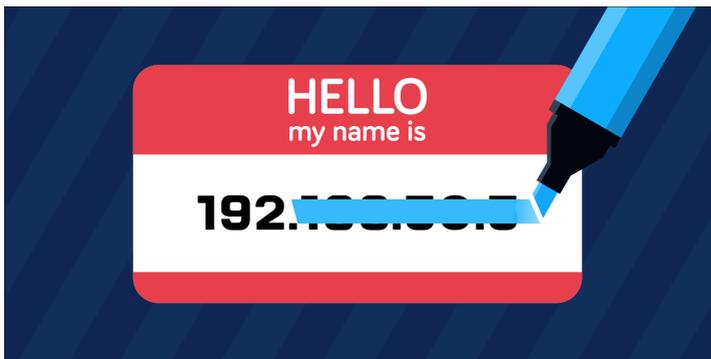
Die Geräte zur Erfassung der Daten für forensische Analysen müssen stets die jeweils geltenden Vorschriften sowie die interne Compliance-Richtlinie einhalten. Das führt oft zu Spannungen zwischen den Abteilungen für Sicherheit und Überwachung des Netzwerks, die die größtmögliche Menge an Informationen für spätere Analysen speichern wollen, und der Rechtsabteilung, die die Gesetzeskonformität des Unternehmens sichern möchte.

Eines der Hauptprobleme, die dabei entstehen, ist die Speicherung der IP-Adressen, die von der DSGVO als personenbezogene Daten angesehen werden, gleichzeitig aber für die Sicherheitsteams unerlässlich sind, um die Informationen zurückverfolgen zu können.

Das andere große Streitthema sind die Daten, die in den Nutzdaten der Pakete gespeichert sind. Diese Informationen sind oft vertraulich und dürfen daher nicht in den Erfassungsgeräten gespeichert werden.

Zudem helfen Mechanismen, mit denen kontrolliert werden kann, welche Informationen gespeichert werden, bei der Kontrolle der Speicherkapazität der Lösung und somit deren Kosten.

SCHEMA:



EINHALTUNG DER DSGVO IN DER FORENSIK

LÖSUNG:

Die Kombination der Slicing/Advanced Slicing und Masking-Aktivitäten behebt die Problematik zwischen den IT- und Rechtsabteilungen.

Zum einen können wir Informationen verschleiern, die vertraulich und daher nicht speicherbar sind. Die Flexibilität der Gigamon Lösung ermöglicht es uns zum Beispiel, nur das letzte Oktett der IP-Adresse unkenntlich zu machen, damit die Informationen verschleiert, aber nicht komplett gelöscht sind, um später forensische Analysen durchführen zu können.

In Kombination mit der Funktion zur Trunkierung der Pakete (Slicing) oder fortgeschrittenen Trunkierung können wir jene Felder löschen, die nicht nützlich sind oder, die die Rechtsabteilung uns nicht erlaubt, wie zum Beispiel Nutzdaten, um so die Sicherheitsrichtlinien einzuhalten und gleichzeitig die Menge an Informationen, die wir speichern, drastisch zu reduzieren und dadurch die Kosten der Erfassungslösung zu senken.

LIZENZEN:

- Slicing
- Advanced Flow Slicing
- Masking