Compliance Monitoring Issues

General Information

In the world of website compliance, a lot of differnt compliance violotions can occour. Therefore we decided to make a clear separation of those violations and introduced different violation categories:

- Regulatory Violations
- Business Violations

Each category includes different types of violations that will be described in the corresponding section. The main differences are that regulatory violatens based on GDPR context prescribed by law and business violations based on custom rules that can be individually defined to meet each customers individual requiremnts.

Regulatory Violations

This category includes all detected problems that relates to the acutal GDPR context prescribed by law. The following types can be detected by the Nimbusec compliance monitor in the context of regulatory violations:

- Cookie Opt-In Generally, the Nimbusec Complaince Scan simulates a standard website user that visits a website, but does not perform any kind of interaction with it (e.g. allowing cookies, ...). For this vioaltion type, we collect all cookie information that was set from the website (before any kind of user interaction). This results in a clear list of cookies that were initially set/provided by the website. In the default configuration, if our simulated website user gets any kind cookies, a 'Cookie Opt-In' violation will be triggerd and shown in the compliance monitor. With other words, cookies have been set without asking for consent in the cookie banner.

In the Nimbusec Compliance Monitor, this violation type can be seen in the compliance view of an asset:

Cookie IssuesComplaince View

By clicking on the "Details" button, all detected cookies can be seen.

Complaince View

If a Cookie Opt-In violation is detected, the following information will be saved.

In more detail, the Nimbusec compliance scan saves the following data:

Example:

Name	Domain	Secure	HttpOnly	LifeTime	SameSite	ThirdParty	InServerResponse
cookie_name	www.example.com	false	false	-1	N/A	true	false

Description of the fields:

Column	Description
Name	Name of the detected Cookie
Domain	Domain name where the described cookie was found
Secure	The Secure flag is an option that can be set by the server when sending a new cookie to the user in an HTTP response. The purpose is to prevent cookies from being observed by unauthorized parties due to sending the cookie in clear text.
HttpOnly	The HttpOnly flag is an additional security option for cookies. If this flag is set, the browser does not display the cookie through client-side scripts.
LifeTime	This parameter shows the validity of a cookie.
SameSite	The SameSite attribute shows if this cookie is restricted to a first-party or same-site context.
ThirdParty	This attribute shows if this cookie was distributed from the own web ressource or from an external one. (domain name matching)

Column	Description
InServerResponse	If the value of this attribute is true, this cookie was directly send from the server. If this value is false, the cookie was created and distributed via a JavaScript context.

- Cookie Banner (ToDo) The Nimbusec Compliance Scan checks websites for the presence of a standard cookie banner. For this case, we check for a default set of various cookie banner implementations. If a custom cookie banner is used, the scan configuration has to be adjusted to detect non default cookie banners.
- Form: HTTP-Transmit For this case, our scan checks all availabe input forms that handles sensitive data. If the content of the input form will be send unencrypted (via HTTP), the Nimbusec Compliance Scan throws a Form: HTTP-Transmit violation. Unencrypted data transmission may be intercepted and the data could be seen in plain text.

By clicking on the "Details" button in the compliance view, all detected cookies can be seen.

Form issues

Complaince View

Complaince View

- Form: Form-Sensitive As mentioned above, the Nimbusec Complaince Scan checks all availabe input forms that handles sensitive data. If we detect such forms, a Form-Sensitive event will be triggered. This should help the users to identify those forms and may handle them in a different way.

Complaince View

- Form: External-Transmit This type of violation gets triggerd if form data will be send to an external processor (e.g. to an external company that may performs user analytics tasks)

Complaince View

Imprint Link Check

- Imprint Policy: The presence of an imprint is a mandaroty regulation in GDPR. Our imprint policy checks the presence of an imprint link on the corresponding website. To detect it, we use predefined search patterns and apply them on the websites source code.

By clicking on the "Details" button in the compliance view, all detected cookies can be seen.
Complaince View

Complaince View

Privacy Policy Link Check

- Privacy Policy: The presence of a privacy statement is a mandaroty regulation in GDPR. Our privacy policy checks the presence of a privacy statement link on the corresponding website. To detect it, we use predefined search patterns and apply them on the websites source code.

Complaince View

Tracker Check

- Tracker: From our point of view, a tracker is any kind of software that collects or transmits data to an external ressource. Therefore, our Nimbusec Compliance Scan analyses the whole network traffic that is active during our simulated website user visits the site. From the GDPR point of view, before the user accepts the defined privacy policy, any kind of data collection or data transmission to third party systems is a violation against the given law.

Revision #1
Created 2021-03-04 08:48:36 UTC by Christian Baumgartner
Updated 2021-03-04 08:54:10 UTC by Christian Baumgartner