Agenda - GDPR and third party JS - can it be done?

- Third party scripts - what are they? Why do we use them?
- Where is the problem?
- Third party security and privacy (OR) a bad inheritance
- GDPR - which part pf the beast are we talking about?
- What can we do about it?
- Why are we still exposed?
- Suggested solution
What are third party scripts?
Third-party scripts

What are they and why do we use them?

- Google Analytics
- DoubleClick by Google
- Facebook
- Adobe Analytics
- OpenX
- Dynamic Yield
- Twitter
- AppNexus
- Optimizely
- LivePerson
Where is the problem?
Third-party scripts

Where is the problem?

Not secured or monitored

- Analytics server
- Social media server
- Ad server
- Forth-Party Ad Server

Secured

- Website Server
- Firewall / WAF

SSL
Third party security and privacy (OR) A bad inheritance

“85% of the exploits detected at in recent years were of third-party plug-ins”

“71% of compromise victims did not detect breaches themselves”

“Median number of days from initial intrusion to detection 87 days”

“Trustedwave Global Security”
The big stores that track your every online move

Holiday shopping with Big Brother is always a bummer.
The “temporary security intrusion” lasted for about 28 hours, the notice said, and it’s believed that names, billing ZIP codes, delivery addresses, email addresses and payment card information — meaning account number, expiration date and CVV number — were compromised.

Pizza Hut emailed thousands of customers this weekend to tell them they may have been impacted by a security breach.

Roughly 60,000 people were impacted.
How does it relate to the GDPR?
Which part of the beast are we talking about?

The right to rectification
A website must provide the user with the option to correct any information stored on him/her or provide a new statement.

The right to be forgotten
A user has the right to request the immediate deletion of all information stored on him/her.

The right to restriction of processing
A user has the right to object to the processing of his/hers personal information.
The blame game (OR) is it my reasonability?

The controller(*) shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient (**) to whom the personal data have been disclosed.

* The controller - the website
** Recipient – a third party vendor
What we can do about it?
## iFrames and the HTML 5 iFrame sandbox

### Pros:
- Isolation from the page
- Some measure of privacy
- Latency protection

### Cons:
- Isolation from the page
- Some third-parties will not run in it

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent top-level navigation</td>
<td>Block script execution</td>
</tr>
<tr>
<td>Block form submission</td>
<td>Disable APIs</td>
</tr>
</tbody>
</table>
What we can do about it

HTTP headers

**Pros:**
- Content source control
- Secure content only

**Cons:**
- Might block third party operation
- Affects the entire page, not only the third party

[CSP] [x-frame-options] [HSTS] [Set-Cookie]
What we can do about it

JS libraries

**Pros:**
- High level of control
- Completely block harmful operations

**Cons:**
- High cost of deployment and maintenance
- Requires tailor made code by either the site or third party
Why are we still exposed?
What we can do about it

Why the low adoption rate?

Implementation and management

Need for speed and flexibility

Need for security and privacy

R&D

Marketing

Security team

$\$\$\$
Friction!!!

Visitor Privacy
Suggested solution
Suggested solution

Making adaption feasible

A policy based system that will easily identify third party scripts and allow the security team complete control over their read/write access, while staying transparent to the third parties and marketing team.
Suggested solution

Making adaption feasible

- Speed and flexibility, let me make $$$
- Give me full control
- Require no adaptation on my side
- Easy implementation, low/no maintenance
Avital Grushcovski
+972-54-222-8380
avital@sourcedefense.com