OWASP
Open Web Application Security Project

OWASP Geneva Chapter meeting
3 décembre 2019

Meeting sponsor

Bienvenue

- Agenda
  - 12h00 Ouverture
  - 12h15 **Industrialisation de la modélisation des menaces un retour d'expérience**
    par: M. Stéphane Adamiste (SCRT)
  - 13h15 Fin
- Conférence
- Après l'événement:
  - Nous suivre: mailing list / calendrier / @owasp_geneva

News

- Fuites de données nov. 2019
- Amendes RGPD: sept. à nov. 2019
- Factorisation RSA
- Bonus: conseils pour lutter contre le phishing

Fuites de données – Nov. 2019

- Florida blue (8.11.2019, 55'000)
- Solara (13.11.2019, 117k)
- Choice cancer care (15.11.2019, n.c.)
- Liver Wellness (17.11.2019, n.c.)
- Adele House (17.11.2019, n.c.)
- Disney (19.11.2019, >2'000)
- Hôpital U. de Rouen (21.11.2019, >3'000)
- Oneplus (22.11.2019, n.c.)
- Florida student (25.11.2019, n.c.)
- Youth development (26.11.2019, n.c.)
- T-Mobile (26.11.2019, 1.1mio.)
- Upbit (27.11.2019, n.c.)
- Ivy Rehab (28.11.2019, n.c.)

Source:
https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-november-2019-1-34-billion-records-breached

"We take data breaches very seriously, and while we do not believe our members' personal information was compromised, we are working closely with Magellan to make sure our potentially impacted members have access to credit monitoring and identity theft protection tools to help them ensure their information is protected."

RGPD: quelles amendes depuis septembre 2019?

(10.09) Morele.net - Mesures insuffisantes (Art. 32 GDPR) eur644,000
(17.09) n.c. - Non respect des principes fondamentaux (Art. 5) eur10,000
(19.09) Delivery Hero - Non respect des droits des utilisateurs (Art. 15) eur195,407
(26.09) Intelligo Media - Bases légales insuffisantes pour le traitement (Art.6) eur9,000
(01.10) Vueling airlines - Bases légales insuffisantes pour le traitement (Art.6) eur30,000
(07.10) Opérateur télécom n.c. - Non conformité avec principes généraux (Art.21 et 25) eur200,000
(07.10) Opérateur télécom n.c. - Non conformité avec principes généraux (Art.21 et 25) eur200,000
(09.10) Vrau Credit SRL - Mesures insuffisantes (Art. 32 GDPR) eur20,000
(09.10) Banque Raiffeisen - Mesures insuffisantes (Art. 32 GDPR) eur150,000
(16.10) ClickQuickNow - Non respect des principes fondamentaux (Art. 5) eur47,000
(16.10) Iberdrola Clientes - Manque de coopération avec l'autorité de supervision (Art. 31) eur8,000
(16.10) Xfera moviles - Bases légales insuffisantes pour le traitement (Art.6) eur60,000
(17.10) Uttis industries - Non respect du devoir d'information (Art.12,13,5c) eur2,500
(18.10) Mairie de Aleksandrów - Politique de protection des données incomplète (Art.28) eur9,380
(23.10) Austrian Post - Bases légales insuffisantes pour le traitement (Art.6) eur18,000,000
(25.10) Vodafone Espana - Bases légales insuffisantes pour le traitement (Art.6) eur36,000
(30.10) Deutsche Wohnen - Non respect des principes fondamentaux (Art. 5) n.c.
(30.10) Deutsche Wohnen - Non respect des principes fondamentaux (Art. 5,Art.25) eur14,500,000
(31.10) UWV (assurance accidents pro.) - Mesures insuffisantes (Art. 32 GDPR) eur900,000
(31.10) Jocker Premium invex - Bases légales insuffisantes pour le traitement (Art.6) eur6,000
(01.11) n.c. - Bases légales insuffisantes pour le traitement (Art.6) eur150,000
(06.11) Cerrajero Online - Non respect du devoir d'information (Art.13) eur1,500
(07.11) Todotecnicos24h - Non respect du devoir d'information (Art.13) eur900
(13.11) CGT - Bases légales insuffisantes pour le traitement (Art.6) eur3,000
(14.11) Telefonica - Non respect des principes fondamentaux (Art. 5) eur30,000
(19.11) Xfera moviles - Mesures insuffisantes (Art. 32 GDPR) eur60,000
(19.11) COrporacion radiotelevision espanola - Mesures insuffisantes (Art. 32 GDPR) eur60,000
(21.11) Futura internationale - Non respect des droits des utilisateurs (Art. 5,6,13,14,21) eur500,000
(21.11) Viqua Xestion Integral - Bases légales insuffisantes pour le traitement (Art.6) eur60,000
(22.11) BNP Paribas - Non respect des droits des utilisateurs (Art. 12,17) eur2,000
(25.11) Courier services company - Mesures insuffisantes (Art. 32 GDPR) eur11,000

TOTAL: € 35 905 687.00

Factorisation RSA

- Nouveau record de factorisation de clés RSA: 795 bits.
- Temps de calcul nécessaire: 100 années (avec 1 cœur de dernière génération) ou 1 jour (avec un processeur doté de 365 cœurs)
- https://arstechnica.com/information-technology/2019/12/new-crypto-cracking-record-reached-with-less-help-than-usual-from-moores-law/

<Last slide>

Date du prochain meeting:
~février 2020

Où trouver de l'info:

- https://www.owasp.org
- https://www.owasp.org/index.php/Geneva
- Twitter: @owasp_Geneva

- Et si vous passez par Zurich:
  https://www.owasp.org/index.php/Switzerland

Joyeuses fêtes à toutes et tous et un grand merci à notre sponsor 2019!

DANS 1 MINUTE…

Industrialisation de la modélisation des menaces un retour d'expérience

Stéphane Adamiste

@sadamiste

sonarsource

Meeting sponsor

OWASP Open Web Application Security Project

sonarsource

Meeting sponsor

OWASP
Open Web Application Security Project

Qui veut gagner des ~~millions?~~ Une sacoche?

Dans la liste ci-après, quelle expression n'a/n'ont pas été utilisée par le conférencier?

1. …des menaces que l'on va éliciter…
2. …renommé «socle de sécurité» par le préposé fédéral…
3. …résultant en une liste pléthorique…
4. …un exercice éminemment intéressant…

Qui veut gagner des ~~millions?~~ Une sacoche?

Dans la liste ci-après, quelle expression n'a/n'ont pas été utilisée par le conférencier?

1. ~~…des menaces que l'on va éliciter…~~
2. …renommé «socle de sécurité» par le préposé fédéral…
3. ~~…résultant en une liste pléthorique…~~
4. ~~…un exercice éminemment intéressant…~~

Qui veut gagner des ~~millions?~~ Une sacoche?

Quelle entreprise a sponsorisé la salle pour tous nos meetings de 2019?

1. SonarSource
2. SonarCode
3. SonarCube

Qui veut gagner des ~~millions?~~ Une sacoche?

Quel a été notre sponsor pour nos meetings de 2019?

1. SonarSource
2. ~~SonarCode~~
3. ~~SonarCube~~