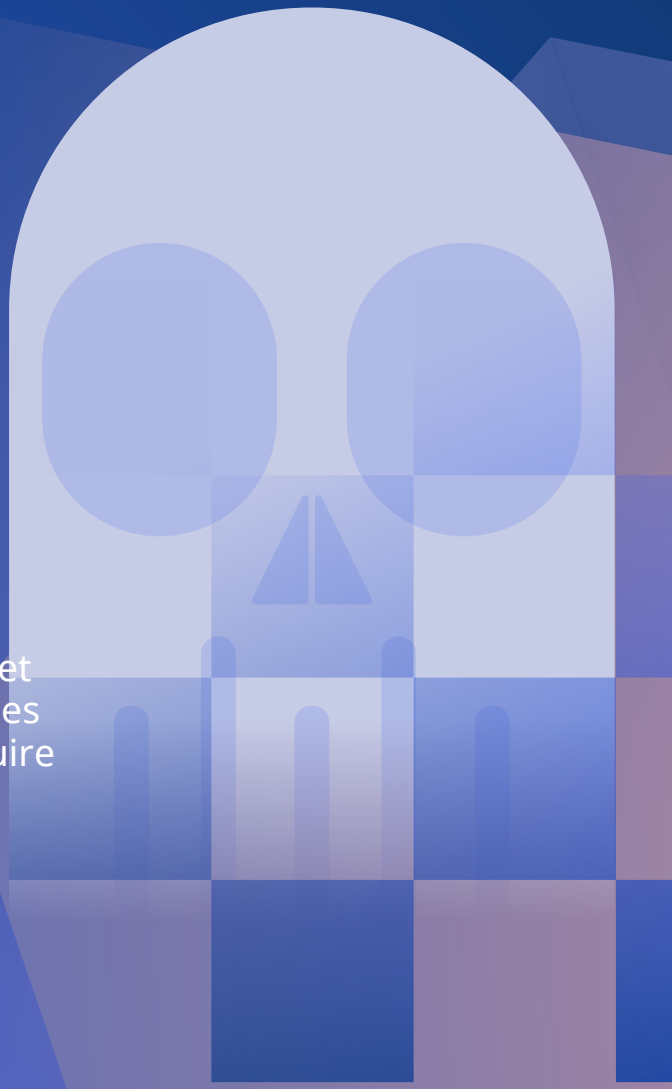
reflectiz

Etude de cas :

LE RISQUE DE PIXELS OUBLIES



Alors que les cyberattaques sur les sites Internet reçoivent beaucoup d'attention, il y a des risques souvent non pris en compte qui peuvent conduire les entreprises confrontées à des poursuites judiciaires pour violations de la vie privée même en l'absence d'incidents de piratage.

L’étude suivante porte sur un de ces cas.

Résumé

Cette étude de cas explore le risque important que posent les pixels de suivi oubliés dans le secteur de la santé. Elle aborde l'introduction de la technologie pixel sur les sites Web, l'importance de se conformer aux réglementations en matière de soins de santé telles que la HIPAA, ainsi qu'à d'autres réglementations en matière de confidentialité telles que le CCPA et le RGPD, et présente une étude de cas récente dans laquelle un fournisseur de services de marketing externe a involontairement exposé des données sensibles de patients. à cause d'un pixel oublié.

Qu'est-ce qu'un pixel de suivi ?

Un pixel de suivi est un petit morceau de code JavaScript conçu pour capturer des données spécifiques sur les visiteurs de votre site Web, que vous pouvez ensuite exploiter pour optimiser l'expérience utilisateur et orienter vos efforts de publicité en ligne. Les pixels de suivi sont méticuleusement conçus pour recueillir des informations précises sur les visiteurs de votre site Web, répondant ainsi aux intérêts spécifiques du spécialiste du marketing.

La technologie Pixel sur les sites Web

Le paysage numérique a considérablement évolué ces dernières années, les sites Web devenant la principale interface entre les organisations et leurs parties prenantes. Naturellement, les propriétaires de sites Web souhaitent maintenir l’engagement de leurs utilisateurs, c’est pourquoi la grande majorité utilise désormais des pixels de suivi pour améliorer l’expérience de leurs utilisateurs. Ces extraits de code permettent aux organisations de surveiller les comportements de leurs utilisateurs, suivre leurs préférences et optimiser leurs efforts marketing. Les pixels des principales plateformes comme Meta (anciennement Facebook et TikTok sont largement utilisés à ces fins.

Etude de cas : un pixel oublié expose la PHI (Patient Health Information)

Dans cette étude de cas, nous explorons un incident alarmant impliquant un fournisseur de services de marketing externe et un site Web de premier plan sur les soins de santé.

L'histoire commence il y a quatre ans, lorsque le fournisseur de services marketing a mené une campagne marketing pour l'organisme de santé, intégrant des pixels de suivi sur son site Web pour surveiller les interactions des utilisateurs. Cependant, après la fin de la campagne, le fournisseur a commis une malheureuse erreur. Il a négligé de supprimer le pixel de suivi du site Web.

Au cours des quatre années suivantes, le site Web de l'établissement de santé a subi des changements importants, notamment l'ajout de nouveaux sous-domaines. À l'insu de tous, le pixel oublié a continué à fonctionner silencieusement en arrière-plan, collectant des données sur le site Web, y compris des informations sensibles sur la santé des patients (PHI). Cette collecte de données par inadvertance est passée inaperçue jusqu'à ce que Reflectiz, un fournisseur proactif de solutions de sécurité de sites Web, identifie la présence du pixel et a sonne l'alarme.

Le risque de dérive de configuration

L'un des dangers potentiels des scripts de suivi est que des erreurs de configuration peuvent leur donner accès à des sous-domaines restreints sur un site ou à d'autres zones où ils ne sont tout simplement pas nécessaires. Même avec les en-têtes de politique de sécurité du contenu (CSP) en place, des fuites peuvent toujours se produire. Par exemple, si Google Tag Manager reçoit l'autorisation, il peut accorder l'accès à d'autres scripts enfants comme le méta-pixel, leur ouvrant ainsi la porte à la collecte de données sensibles protégées.

La solution Reflectiz a permis à l'équipe de sécurité des informations de ce prestataire de soins d'identifier le pixel malveillant, ainsi que le système de gestion des balises avec lequel il a été mis en œuvre, et d'empêcher toute nouvelle fuite de données. Cette intervention réussie a attiré l'attention sur la nécessité urgente de mettre en œuvre une procédure interne qui empêcherait que ce type de désastre prolongé en matière de données ne se reproduise.

La détection de la fuite de données par Reflectiz a également attiré l'attention de l'équipe sur la nécessité de restreindre les privilèges d'accès aux campagnes et aux pixels de suivi des fournisseurs de marketing numérique externes à l'avenir. Il faudrait les empêcher d'accéder à des sous-domaines, pages, chemins et champs de saisie utilisateur protégés contenant des informations personnelles et des données personnelles. Il serait essentiel d'imposer des restrictions à ces zones pour les empêcher de collecter involontairement des données aussi sensibles à l'avenir.

Reflectiz peut détecter les modifications non autorisées et déclencher des alertes même lorsque les scripts sont correctement configurés mais affichent des comportements modifiés ou problématiques. Il peut faire de même lorsque la dérive de la configuration (modifications ad hoc du logiciel ou du matériel) crée également des changements de comportement.

PIXELS DE SUIVI VS. COOKIES

Les pixels de suivi sont intégrés dans les e-mails et les pages Web, tandis que les cookies sont des fichiers stockés sur l'appareil d'un utilisateur. Pour faire simple, les pixels sont le moteur du placement de cookies sur votre ordinateur. Alors que les pixels de suivi étaient initialement des images, ils ont depuis évolué vers des extraits de script plus sophistiqués. L'intégration de ces scripts est une tâche complexe qui nécessite de solides compétences en programmation. Grâce aux scripts, les pixels de suivi peuvent transmettre un plus grand volume d'informations que leurs homologues basés sur des images.

Règlements sur les soins de santé - HIPAA

Dans le secteur de la santé, où la confidentialité des données des patients est primordiale, des réglementations telles que la Health Insurance Portability and Accountability Act (HIPAA) sont en place pour protéger les informations sensibles des patients. La HIPAA établit des normes strictes en matière de sécurité et de confidentialité des données, obligeant les organismes de santé à mettre en œuvre des mesures de protection pour protéger les informations électroniques sur la santé (PHI). Les violations de la HIPAA peuvent entraîner de graves conséquences, notamment de lourdes amendes et une atteinte à la réputation.

Structure des pénalités HIPAA 2023

The HIPAA Journal

Niveau 1
Une violation dont l'entité couverte n'était pas au courant et n'aurait pas pu être évitée de manière réaliste si des précautions raisonnables avaient été prises pour respecter la règle HIPAA.s

Pénalité par violation
$137 - $68,928

Niveau 2
Une violation dont l'entité couverte aurait dû être consciente mais n'aurait pas pu l'éviter même avec un soin raisonnable. (mais sans négliger délibérément les règles HIPAA)

Pénalité par violation
$1,379 - $68,928

Niveau 3
Une violation résultant directement d'une « négligence délibérée » des règles HIPAA, dans les cas où une tentative a été faite pour corriger la violation.

Pénalité par violation
$13,785 - $68,928

Niveau 4
Une violation des règles HIPAA constituant une négligence intentionnelle, pour laquelle aucune tentative n'a été faite pour corriger la violation dans les 30 jours.

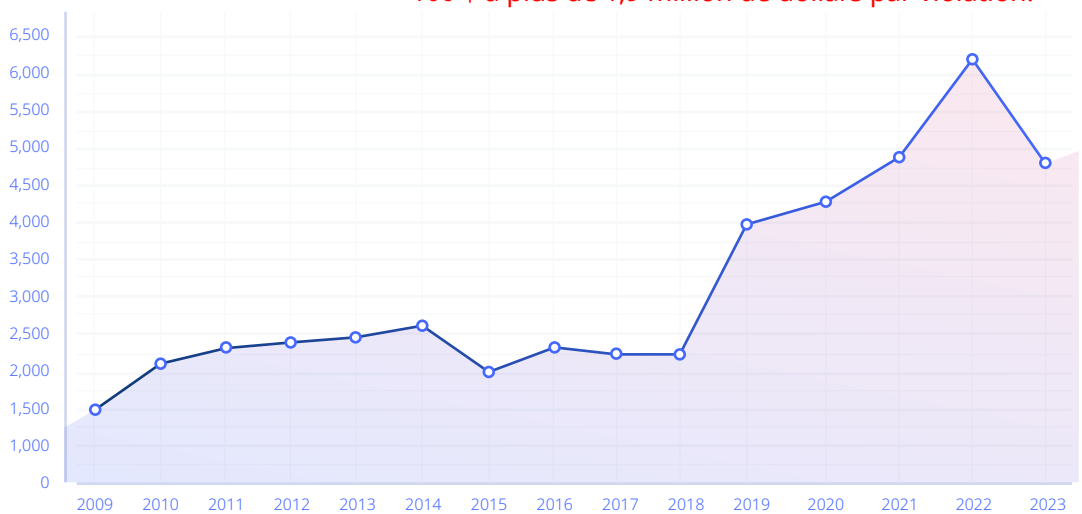
Pénalité par violation
$68,928 - $2,067,813

Prévention des violations du RGPD et de la HIPAA

Étant donné que le RGPD exige que les organisations obtiennent un consentement clair avant de transférer les données des utilisateurs au-delà des frontières nationales, il est également rassurant que Reflectiz puisse bloquer les tentatives de transfert de données personnelles entre juridictions par chaque script ou pixel et alerter les utilisateurs lorsqu'ils tentent. De telles violations peuvent être coûteuses, comme Facebook l'a découvert en 2022 lorsqu'il a reçu une amende de 18 millions de dollars pour avoir autorisé 12 exemples de ce type de violation.

Si l'on considère qu'il est possible d'enfreindre simultanément la HIPAA et le RGPD (si un organisme de santé aux États-Unis traite des citoyens de l'UE et ne protège pas correctement leurs données de santé), le risque d'amendes énormes est accru et la nécessité pour une surveillance continue devient encore plus claire. Le RGPD a fixé une amende maximale de 20 millions d'euros ou 4 % du chiffre d'affaires mondial annuel, selon le montant le plus élevé, et comme le montre le graphique ci-dessus, la HIPAA a établi des sanctions en cas de non-conformité en fonction du niveau de négligence, avec des pénalités allant de 100 $ à plus de 1,9 million de dollars par violation.

Median Data Breach Size
2009 - Aug 2023



Points clés à retenir

A. Confidentialité des données dans le secteur de la santé

Le secteur de la santé doit donner la priorité à la confidentialité et à la sécurité des données, compte tenu de la sensibilité des informations sur les patients. L'exposition accidentelle de PHI en raison d'un pixel oublié souligne l'importance d'une vigilance continue.

C. Conformité avec HIPAA

Les organismes de santé doivent s'assurer que leurs pratiques numériques sont conformes aux réglementations HIPAA. Cela inclut la surveillance des intégrations tierces et le suivi des pixels pour détecter d'éventuelles violations de la vie privée.

B. Gestion des pixels

Les organisations, en particulier dans les secteurs hautement réglementés comme la santé, doivent établir des processus robustes de gestion des pixels. Cela comprend des audits réguliers pour identifier et supprimer les pixels inutiles ou non autorisés.

D. Solutions de sécurité proactives

La capacité de Reflectiz à détecter et atténuer les risques associés aux pixels oubliés montre l'importance de mesures de sécurité proactives. Une surveillance continue et des alertes en temps réel peuvent aider les organisations à identifier et à corriger rapidement les violations potentielles de données.

Comment Reflectiz peut aider

Reflectiz, un leader de solutions de sécurité pour sites Web, propose une approche proactive de la gestion des pixels et de la sécurité des sites Web. Dans le cas de l'organisation de soins de santé, Reflectiz a joué un rôle central dans l'identification du pixel oublié et dans l'atténuation des risques qui y sont associés.

A. Monitoring continu

Les capacités de monitoring avancées de Reflectiz garantissent que tous les pixels et intégrations tierces d'un site Web sont suivis et analysés en permanence. Cette approche proactive aide les organisations à identifier les violations potentielles de la vie privée en temps réel.

B. Alertes et remédiation

Lorsque Reflectiz a détecté le pixel oublié, il a déclenché des alertes auprès de l'équipe de sécurité de l'établissement de santé. Cela leur a permis de remédier immédiatement au problème, notamment en supprimant le pixel non autorisé et en évaluant les données collectées.

C. Solutions de sécurité personnalisées

Reflectiz adapte ses solutions pour répondre aux besoins spécifiques de chaque organisation, en tenant compte des réglementations du secteur et des risques potentiels. Cela garantit que les organisations travaillant dans des secteurs hautement réglementés, tels que les soins de santé, peuvent maintenir leur conformité tout en maximisant les avantages de leur présence numérique.

D. Reporting complet

Reflectiz fournit des rapports détaillés sur l'état des intégrations tierces d'un site Web, y compris les pixels de suivi. Ces rapports permettent aux organisations de prendre des décisions éclairées sur l'état de sécurité et de conformité de leur écosystème numérique.

En conclusion, cette étude de cas rappelle brutalement les risques associés au marketing numérique et à la technologie de suivi.

Les organismes de santé doivent rester vigilants pour protéger les données des patients et se conformer à des réglementations strictes comme la HIPAA, mais il convient également de rappeler que même sans les problèmes potentiels causés par des oublis aussi simples, ils devraient quand même être plus vigilants que la plupart des autres. En effet, ces dernières années, le secteur de la santé est devenu la principale cible des menaces de cybersécurité, **70 %** de tous les incidents de sécurité des données à grande échelle touchant les prestataires de soins de santé.

L'approche proactive de Reflectiz en matière de gestion des pixels et de sécurité des sites Web offre une solution précieuse pour atténuer tous ces risques et garantir la protection continue des informations sensibles des patients. En donnant la priorité à la confidentialité des données et en adoptant des mesures de sécurité proactives, les organisations peuvent naviguer dans le paysage numérique en toute confiance, protégeant ainsi leur réputation et évitant des violations de conformité coûteuses.

Healthcare Regulations - HIPAA

Rank	Name of Covered Entity	Year	Covered Entity Type	Individuals Affected	Type of Breach
1	Anthem Inc.	2015	Health Plan	78,800,000	Hacking/IT Incident
2	American Medical Collection Agency	2019	Business Associate	26,059,725	Hacking/IT Incident
3	HCA Healthcare	2023	Business Associate	11,270,000	Hacking/IT Incident
4	Premera Blue Cross	2015	Health Plan	11,000,000	Hacking/IT Incident
5	Excellus Health Plan, Inc.	2015	Health Plan	10,000,000	Hacking/IT Incident
6	Managed Care of North America (MCNA Dental)	2023	Business Associate	8,923,662	Ransomware attack
7	PharMerica	2023	Healthcare Provider	5,815,591	Ransomware attack
8	Science Applications International Corporation	2011	Business Associate	4,900,000	Loss

Rank	Name of Covered Entity	Year	Covered Entity Type	Individuals Affected	Type of Breach
9	University of California, Los Angeles Health	2015	Healthcare Provider	4,500,000	Hacking/IT Incident
10	Community Health Systems Professional Services Corporations	2014	Business Associate	4,500,000	Hacking/IT Incident
11	Colorado Department of Health Care Policy & Financing	2023	Health Plan	4,091,794	Hacking/IT Incident
12	Advocate Health and Hospitals Corporation, d/b/a Advocate Medical Group	2013	Healthcare Provider	4,029,530	Theft
13	OneTouchPoint	2022	Business Associate	4,112,892	Ransomware attack
14	Medical Informatics Engineering	2015	Business Associate	3,900,000	Hacking/IT Incident
15	Eye Care Leaders	2022	Business Associate	3,649,470	Hacking/IT Incident
16	Banner Health	2016	Healthcare Provider	3,620,000	Hacking/IT Incident
17	Florida Healthy Kids Corporation	2021	Health Plan	3,500,000	Hacking/IT Incident
18	Trinity Health	2020	Business Associate	3,320,726	Hacking/IT Incident
19	Newkirk Products, Inc.	2016	Business Associate	3,466,120	Hacking/IT Incident
20	Regal Medical Group (including Lakeside Medical Organization, A Medical Group, ADOC Acquisition Co., A Medical Group Inc. & Greater Covina Medical Group Inc)	2023	Healthcare Provider	3,300,638	Ransomware attack
21	20/20 Eye Care Network, Inc	2021	Business Associate	3,253,822	Hacking/IT Incident
22	Cerebral, Inc.	2023	Business Associate	3,179,835	Impermissible Disclosure (website tracking code)
23	NationsBenefits Holdings, LLC	2023	Business Associate	3,037,303	Hacking Incident (Fortra GoAnywhere MFT)
24	Advocate Aurora Health	2022	Healthcare Provider	3,000,000	Impermissible Disclosure (website tracking code)
25	Dominion Dental Services, Inc., Dominion National Insurance Company, and Dominion Dental Services USA, Inc.	2019	Health Plan	2,964,778	Hacking/IT Incident
26	AccuDoc Solutions, Inc.	2018	Business Associate	2,652,537	Hacking/IT Incident
27	Harvard Pilgrim Health Care	2023	Health Plan	2,550,922	Hacking/IT Incident
28	Forefront Dermatology, S.C.	2021	Healthcare Provider	2,413,553	Hacking/IT Incident

Rank	Name of Covered Entity	Year	Covered Entity Type	Individuals Affected	Type of Breach
29	Connexin Software	2022	Business Associate	2,216,365	Hacking/IT Incident
30	21st Century Oncology	2016	Healthcare Provider	2,213,597	Hacking/IT Incident
31	Shields Healthcare Group	2022	Business Associate	2,000,000	Hacking/IT Incident
32	Xerox State Healthcare, LLC	2014	Business Associate	2,000,000	Unauthorized Access/ Disclosure
33	Professional Finance Company	2022	Business Associate	1,918,941	Ransomware attack
34	IBM	2011	Business Associate	1,900,000	Unknown
35	Performance Health Technology	2023	Business Associate	1,750,000	Hacking/IT Incident
36	Dental Care Alliance, LLC	2021	Business Associate	1,723,375	Hacking/IT Incident
37	GRM Information Management Services	2011	Business Associate	1,700,000	Theft
38	NEC Networks, LLC d/b/a CaptureRx	2021	Business Associate	1,656,569	Hacking/IT Incident
39	Baptist Medical Center and Resolute Health Hospital	2022	Healthcare Provider	1,608,549	Hacking/IT Incident
40	Inmediata Health Group, Corp.	2019	Healthcare Provider	1,565,338	Unauthorized Access/ Disclosure
41	Eskenazi Health	2021	Healthcare Provider	1,515,918	Hacking/IT Incident
42	Community Health Network	2022	Healthcare Provider	1,500,000	Impermissible Disclosure (website tracking code)