SITE WEB & CYBERSÉCURITÉ

Connaître les risques
Bien se préparer

ENTRELOUPS
Dev web & mobile depuis 2007

« Rien ne sert d'avoir peur, il faut prendre les devants. » pourrait-on écrire.

Sans tomber dans la paranoïa ni le déni, il faut prendre la question de la sécurité de son site web au sérieux.

Ce guide vous aidera, en tant que propriétaire d'un site web et sans terme technique, à comprendre les enjeux de la sécurité et à aborder cette question sereinement. »

ENTRELOUPS

Dev web & mobile depuis 2007

SOMMAIRE

01

ENTRELOUPS

Dev web & mobile depuis 2007

INTRODUCTION

L'omniprésence du web dans la communication et le business des entreprises induit de nouveaux dangers qu'il faut gérer.

Ce domaine étant avant tout une question de techniciens et de spécialistes, il peut paraître effrayant, abstrait, voire lointain.

Il est important de ne pas avoir vis à vis de la sécurité de son site web la même approche que certains ont avec leur antivirus : en prendre un au hasard ou même ne pas en prendre du tout.

Ici, nous vous parlerons donc, sans détour et sans technique, de la sécurité de votre site web et de ses conséquences.

Il est important de noter [...] que les attaques d'applications Web sont devenues le vecteur numéro 1 des cas de compromissions de données, et que 95% des compromissions d'applis Web avaient des motivations financières. (1)

02

ENTRELOUPS

Dev web & mobile depuis 2007

A PROPOS DES AUTEURS

Depuis 2007, Entreloups conçoit et développe sur mesure des solutions et outils digitaux : e-commerce, applicatifs métiers, app mobiles.

La nature des projets menés a conduit Entreloups a porter une attention toute particulière aux enjeux de la sécurité dans le développement web et mobile.

La sécurité a donc été placée au cœur de nos méthodes de développement autant que dans les échanges et partages de connaissances au sein de l'équipe.

Ce livre blanc s'inscrit dans cette démarche de diffusion et de partage des savoir-faire.

A PROPOS DES AUTEURS

Régis Grison, fondateur d'Entreloups, a 20 ans d'expérience dans les technologies du web. Titulaire d'une Maîtrise d'Informatique, il a commencé sa carrière chez Ubisoft avant d'explorer d'autres horizons et technologies. Avec Entreloups il accompagne aujourd'hui start-ups, PME et grands comptes dans la mise en oeuvre des technologies et contribue à la formation et développement des compétences des membres d'Entreloups.

Stéphane Debeil est diplômé en Informatique et Administration Systèmes et Réseaux. Il rejoint très tôt Entreloups où il met à profit sa passion pour la sécurité informatique. Développeur expérimenté, il a à cœur de diffuser et mettre en oeuvre les bonnes pratiques au sein des équipes qu'il encadre sur ses projets.

03

ENTRELOUPS

Dev web & mobile depuis 2007

MYTHES & RÉALITÉS

Il y a beaucoup d'idées reçues à propos de la sécurité des sites web, tellement, que nous ne pouvions commencer ce livre blanc sans en faire le tour.

1 « MON SITE (OU MA SOCIÉTÉ) N'EST PAS ASSEZ CONNUE POUR ÊTRE UNE CIBLE INTÉRESSANTE »

Absolument toutes les entreprises interrogées [...] ont subi une cyberattaque à un moment ou un autre, dont les deux tiers dans l'année écoulée. (2)

Au contraire, les « petits » sont souvent moins bien protégés et donc des cibles faciles. Ils peuvent ensuite servir au pirate pour attaquer un autre serveur.

2 « JE N'AI JAMAIS ÉTÉ ATTAQUÉ(E) »

Il est très tentant de le dire, surtout pour s'en convaincre. La vérité c'est que la quasi-totalité des sites web subissent des attaques. Certes, la plupart n'aboutissent pas, et c'est heureux, mais il ne faut pas s'imaginer que le pirate va forcément laisser un petit mot pour se signaler, comme nous le verrons plus tard.

Autrement dit, si jamais un pirate arrive à récupérer le contenu de la base de données, aucun signe extérieur ne vous permettra de le deviner.

MYTHES & RÉALITÉS

78% des responsables IT [Ndlr: technologies de l'information, informatique] interrogés déclarent qu'ils ont dû changer leur stratégie de sécurité en 2016, en raison d'une faille de sécurité. Ils n'étaient que 53% en 2014. (3)

3 « MON SITE A ÉTÉ CRÉÉ PAR DES PROFESSIONNELS, IL EST DONC SÉCURISÉ »

Malheureusement, ce n'est pas toujours vrai. Tous les professionnels ne sont pas sensibilisés à la sécurité et tout le monde commet des erreurs.

D'une façon générale, des tests poussés en sécurité prennent du temps, s'ils n'apparaissent pas en toutes lettres dans le détail de la facture, mieux vaut considérer qu'ils n'ont pas été faits.

4 « J'AI FAIT TESTER LA SÉCURITÉ DE MON SITE, IL EST DONC SÛR »

Oui, au moment du test. Le site évolue ensuite, les techniques de piratage également. On peut comparer un test de sécurité web au contrôle régulier des extincteurs : il faut vérifier périodiquement.

MYTHES & RÉALITÉS

5 « J'AI FAIT METTRE UN FIREWALL (PAREFEU) SUR LE SERVEUR »

Le rôle du pare-feu (définition dans le glossaire) est, dans ce cas, de ne laisser passer que les communications avec votre site web. En d'autres termes, tout utilisateur interagissant avec votre site web ne sera pas bloqué par votre pare-feu.

Il existe certes des pare-feu applicatifs qui ont pour rôle de surveiller le contenu des échanges entre le visiteur et le site mais ils sont plus rares et ne garantissent pas à eux seuls une sécurité totale.

6 « LE SITE EST EN SSL (CONNEXION SÉCURISÉE) »

Le SSL (définition dans le glossaire) garantit uniquement que tout échange d'informations entre le serveur et le visiteur de votre site n'est ni lisible ni modifiable par un pirate qui aurait réussi à intercepter la communication. Si le visiteur est le pirate, le SSL ne protégera pas votre site.

MYTHES & RÉALITÉS

CE QU'IL FAUT RETENIR

- La sécurité est une affaire de spécialistes qui concerne tout le monde et qu'il ne faut pas prendre à la légère.
- Il n'existe aucune solution magique et durable. Seuls des audits réguliers peuvent garantir la sécurité à long terme.

04

ENTRELOUPS

Dev web & mobile depuis 2007

QUELS RISQUES ?

Un pirate qui arrive à accéder d'une façon détournée à un site web ou à ses données peut avoir divers buts. A chaque objectif correspond des problèmes différents pour le propriétaire de site web.

1 « LE TABLEAU DE CHASSE »

C'est sans doute un des cas les moins graves, en apparence. Le pirate place un fichier qui prouve qu'il a piraté le site et indique sa « prise » sur un site qui référence les exploits de son groupe.

Même s'il n'était pas mal intentionné, ce dernier attire alors l'attention sur le site piraté, indiquant au monde entier, en tout cas à ceux qui savent où regarder, qu'il existe une vulnérabilité qui peut être exploitée. De gros problèmes peuvent suivre.

92% des entreprises qui ont connu une faille de sécurité dans les cinq dernières années déclarent avoir constaté des conséquences commerciales (retard dans les développements de produits à 36%, mauvaise presse à 30%, baisse de la confiance des clients à 26%). (3)

QUELS RISQUES ?

2 « LA BACKDOOR (PORTE DÉROBÉE) »

Ce cas est plus grave car le pirate laisse sur le serveur des fichiers, en apparence anodins, qui lui permettront de revenir et de faire absolument tout ce qu'il veut sur le serveur. Inutile de préciser qu'il en a l'intention.

Il va attendre suffisamment de temps pour se faire oublier et pour que ses fichiers soient intégrés à d'éventuelles sauvegardes. Là encore, le pire est à venir et le nettoyage du site peut s'avérer complexe.

3 « LE DÉTOURNEMENT DU SITE »

Il peut s'agir ici d'une page cachée utilisée pour du phishing (définition dans le glossaire), de liens vers un site qui rapportera de l'argent au pirate ou d'une simple modification du site pour montrer son passage. Le site peut aussi être utilisé pour de l'envoi de spam.

L'image du site et de l'entreprise est directement impactée si le détournement est visible. S'il n'est pas directement visible, le site peut finir par être coupé suite à des plaintes.

QUELS RISQUES ?

4 « L'ARRÊT DU SITE »

Ici nous commençons à avoir de très sérieux problèmes : le site est en panne (partiellement ou totalement). S'en suivent une perte de fréquentation, une mauvaise image, voire une perte directe de chiffre d'affaire si le site est au cœur de votre activité.

5 « LE VOL DE DONNÉES »

C'est le pire des scénarios : le pirate trouve une faille, parfois simple, et l'utilise pour voler des données. Il peut s'agir des mots de passe administrateurs, du savoirfaire de l'entreprise ou de la base clients. Dans ce dernier cas, la responsabilité pénale du dirigeant de l'entreprise peut même être recherchée. (4)

De plus, selon une étude réalisée pour FireEye (5), 60 % des clients dont les données ont été volées ne feront plus affaire avec l'entreprise qui a été piratée, le même pourcentage envisage même une action en justice contre la société victime du piratage.

QUELS RISQUES ?

On retrouve des motivations financières ou d'espionnage dans 89% de toutes les attaques. (1)

CE QU'IL FAUT RETENIR

- Un site, même en apparence intact peut avoir été compromis.
- Un piratage peut avoir des répercutions financières.
- La responsabilité pénale peut être recherchée par les utilisateurs en cas de vol de données personnelles.

05

ENTRELOUPS

Dev web & mobile depuis 2007

COMMENT FONT-ILS ?

Les pirates ont plusieurs angles d'attaque possible.

Ils peuvent profiter d'erreurs de configuration qui leur donnent des informations. Ils utilisent ensuite ces dernières pour mieux cibler leurs attaques.

Dans 93% des cas, il faut à peine quelques minutes à des hackers pour compromettre des systèmes, et dans 28% des cas ils parviennent à exfiltrer des données en quelques minutes seulement. (1)

Ils peuvent utiliser des failles connues présentes dans le logiciel utilisé par le site. Ces dernières sont généralement publiées et ne posent de problèmes que si le site n'est pas tenu à jour.

Ils peuvent induire en erreur le serveur web afin de le pousser à communiquer des informations qui ne devraient pas l'être. Ils peuvent enfin profiter de failles humaines : un mot de passe trop simple, partagé entre plusieurs utilisateurs, communiqué par téléphone ou par email en pensant avoir affaire à un autre employé, ...

30% des incidents sont attribuables à l'erreur humaine. Pour les fuites de données, le chiffre tombe à seulement 10%. (7)

Ce qu'il faut retenir :

- Les pirates profitent souvent de l'erreur humaine.
- Les logiciels doivent être mis à jour.
- Il existe des techniques visant à détourner le système.

06

ENTRELOUPS

Dev web & mobile depuis 2007

COMMENT SE PROTÉGER ?

L'équipe qui gère le site sera une cible privilégiée pour les pirates. Il convient donc de la former et de la sensibiliser à la sécurité. Il est nécessaire d'utiliser de bons mots de passe, de ne jamais les divulguer ni les réutiliser, de donner à chaque membre de l'équipe les privilèges dont il a besoin mais pas plus. Il faudra également sensibiliser l'équipe aux risques habituels de l'informatique et d'internet : phishing, virus, ...

63% des compromissions de données avérées sont imputables à l'utilisation de mots de passe volés, faciles à deviner ou de mots de passe par défaut qui n'ont pas été modifiés. (1)

L'équipe de développement, qu'elle soit interne ou non, devra également être sensibilisée aux bonnes pratiques : une grosse partie des risques peut être évitée par l'application de principes simples. L'idéal reste de former les développeurs en amont de la création du site mais il n'est jamais trop tard pour prendre de bonnes habitudes et corriger des failles.

99,9% des vulnérabilités des systèmes sont exploitées plus d'un an après avoir été identifiées [faute de mise à jour]. (7)

Si le site utilise un logiciel qui n'est pas développé sur mesure, qu'il s'agisse ou non d'un logiciel libre, il conviendra de faire les mises à jour de sécurité dès que possible, pour le logiciel comme les modules.

COMMENT SE PROTÉGER ?

Il existe souvent des modules complémentaires qui peuvent améliorer la sécurité du site.

La configuration du site est importante également. Sans rentrer dans les détails techniques, une mauvaise configuration peut fournir des informations au pirate ou même lui permettre d'accéder à des zones sensibles du site.

L'administration du serveur est tout aussi importante. Un serveur mal administré peut ouvrir des portes aux pirates alors que le site web lui-même serait fiable. Les points importants sont :

- La configuration générale pour éviter de communiquer trop d'informations et de laisser des fonctionnalités inutiles accessibles
- Les contremesures pour rejeter les tentatives de piratage
- Les mesures de détection pour identifier les attaques les plus sérieuses, celles qui peuvent éventuellement avoir abouti
- Les mises à jour

Parce qu'il faut prévoir les situations de crise, il faut faire des sauvegardes fréquentes tout en gardant une version qui n'a jamais été mise sur internet (pour la recherche de modifications par un pirate discret). Il convient également de préparer une procédure de reprise suite à incident (voir le glossaire) afin de pouvoir remettre le site en marche le plus rapidement possible en cas de problème or 52% des entreprises n'en ont pas (2).

COMMENT SE PROTÉGER ?

De plus en plus d'assurances proposent des contrats de cybersécurité qui vous assisterons dès le piratage du site, faisant appel à des experts, en plus de l'indemnisation éventuelle.

Enfin, il est important de faire auditer régulièrement la sécurité de son site par des experts.

Ce qu'il faut retenir :

- Il faut former vos équipes : celles qui développent et celles qui gèrent le site.
- Utilisez des modules de sécurité lorsqu'ils sont disponibles.
- Configurations et mises à jour sont essentielles.
- Ne négligez pas l'administration du serveur.
- Il faut se préparer au pire (plan de reprise, sauvegardes, ...)
- Il faut faire auditer régulièrement la sécurité de son site web.

07

ENTRELOUPS

Dev web & mobile depuis 2007

QUE FAIRE APRÈS UN PIRATAGE ?

Si vous avez souscrit une assurance cybersécurité, il faut la contacter en premier lieu. Cette dernière peut comprendre une assistance à la gestion de la crise qui peut couvrir les domaines techniques, juridiques, ainsi que la relation clients.

Côté technique, c'est à ce moment que le plan de reprise est activé. Cela comprend la recherche de la faille de sécurité utilisée par le pirate et la remise en marche du site.

Si le pirate a pu prendre le contrôle du site une fois, il pourra recommencer et le fera certainement dans un très bref délai. Il faut donc découvrir comment il a pris le contrôle du site et supprimer l'accès sans délai. Une copie de sauvegarde qui n'a jamais été mise en contact avec internet peut être d'une grande utilité pour cela.

La découverte d'une cyberattaque prend, dans plus des deux tiers des cas, entre un et six mois. Et l'entreprise met un temps similaire à se remettre en état. (2)

Une fois le site à nouveau sûr, il est important de le remettre en marche pour limiter les pertes pour l'entreprise.

Cette étape est plus complexe qu'une simple restauration de sauvegarde car il faut que le site restauré soit à la fois à jour et sain.

QUE FAIRE APRÈS UN PIRATAGE ?

Sur le plan judiciaire, le pirate est passible de grosses peines. Il est possible de porter plainte auprès de la police, de la gendarmerie ou du procureur de la république (par écrit).

Les informations présentes sur le serveur permettront à la justice d'identifier l'auteur du piratage.

Il faut malgré tout préciser que le monde virtuel évolue plus vite que le monde physique et que les procédures judiciaires ont parfois du mal à franchir les frontières de certains pays. Cette situation est malgré tout en train d'évoluer dans le bon sens et "87% des cyberattaques en France auraient été perpétrées par des hackers basés dans le pays." (12)

Jusqu'à mai 2018, le code pénal obligeait seulement les "fournisseurs de services de communications électroniques" à informer la CNIL en cas de vol d'une base de données contenant des informations à caractère personnel (5) (sauf si cette dernière est chiffrée (8 et 9)).

A partir de mai 2018, cette obligation a été étendue à l'ensemble des entreprises (RGPD)

.44 % des entreprises européennes ont subi un vol de données au cours des douze derniers mois. (11)

En cas de vol de données, il est obligatoire de prévenir la CNIL dans les 72 heures en l'informant des mesures qui auront déjà été prises pour que le problème ne se reproduise pas.

QUE FAIRE APRÈS UN PIRATAGE ?

Cette dernière pourra imposer de prévenir les personnes concernées par le vol de données (10 et 13).

La communication avec vos clients quand il s'agit d'un vol de données à caractère personnel reste un point important, notamment pour votre image. Quand une base est vendue, il est généralement fait mention de sa provenance et tout peut finir par se savoir. La transparence est au moins une option à étudier.

Ce qu'il faut retenir :

- Contactez sans attendre votre assurance si vous avez souscrit un contrat cybersécurité.
- Remettre en marche un site piraté est une opération complexe.
- Portez plainte contre les pirates.
- Si la base client est volée, vous devez agir et prévenir la CNIL.

08

ENTRELOUPS

Dev web & mobile depuis 2007

CONCLUSION

Personne n'est trop insignifiant pour être attaqué par un pirate. Pour autant, la plupart du temps, ces derniers n'obtiennent rien. Certains testent donc un très grand nombre de sites web en espérant en trouver un par hasard qui n'est pas bien sécurisé. Ne soyez pas celui-là !

Une bonne politique de sécurité, des mises à jour régulières et des vérifications par des spécialistes sont autant de gages que votre site web pourra fonctionner comme vous l'attendez.

Si vous avez une équipe de développement, qu'elle soit interne ou non, ne négligez pas leur sensibilisation à la sécurité. Une formation courte peut leur donner des clés pour éviter les principales erreurs.

Même si la sécurité est assurée d'un point de vue technique, il est tout aussi important de sensibiliser l'équipe qui gère le site.

Et surtout : préparez-vous et faites vérifier périodiquement votre site.

DES DOUTES ? DES QUESTIONS ?

06 95 56 38 62

infos-clients@entreloups.com

09

ENTRELOUPS

Dev web & mobile depuis 2007

GLOSSAIRE

Pare-feu : logiciel permettant de filtrer les tentatives de connexions venant de l'extérieur. Le blocage peut être sélectif.

Phishing : aussi appelé "hameçonnage", technique qui consiste à se faire passer pour une personne ou un organisme de confiance afin d'obtenir de l'argent ou des informations. Le moyen utilisé peut être un email, un faux site web, un appel téléphonique, un SMS, ...

Procédure de reprise suite à incident : aussi appelée "plan de reprise d'activité". Cette procédure définit la suite d'actions à réaliser pour remettre en service un système informatique dans les plus brefs délais suite à un incident (panne, piratage, ...). Elle peut également définir les mesures préventives à prendre en amont (mise en place d'une politique de sauvegardes, formation du personnel, procédures de sécurité, ...)

SSL : en anglais "Secure Sockets Layers", connexion sécurisée entre un visiteur et un site web. On l'identifie généralement par un cadenas dans la barre d'adresse ou en bas à droite du navigateur, ainsi que par la mention « https » dans l'adresse du site. La connexion sécurisée garantit qu'il n'est pas possible d'intercepter ni d'écouter les conversations mais ne garantit pas que l'interlocuteur est honnête, contrairement à ce qu'on lit parfois.

RÉFÉRENCES

(1) https://www.lenetexpert.fr/socialengineeringlescybercriminelsprofitentdelanaturehumaine-datasecuritybreachdatasecuritybreach/

(2) https://www.cioonline.com/actualites/lire100desentreprisesonttentelescybercriminels-7722.html

(3) https://www.frenchweb.fr/10chiffresquimontrentquelesentreprisesneprotegentpas-suffisammentleursdonnees/246299

(4) https://www.legifrance.gouv.fr/affichTexteArticle.do?idArticle=LEGIARTI000006528132&cidTexte=LEGITEXT000006068624

(5) https://www.cnil.fr/fr/lessanctionspenales

(6) https://www2.fireeye.com/rs/848DID242/images/rptbeyondbottomline.pdf

(7) http://www.usinedigitale.fr/article/lacomplexificationdescyberattaquesen8 chiffres.N339067

(8) https://www.legifrance.gouv.fr/affichTexteArticle.do?idArticle=LEGIARTI000025620398&cidTexte=LEGITEXT000006052581

(9) https://www.legifrance.gouv.fr/affichTexteArticle.do?idArticle=LEGIARTI000025620401&cidTexte=LEGITEXT000006052581

(10) https://www.legifrance.gouv.fr/affichTexteArticle.do?idArticle=LEGIARTI000025620405&cidTexte=LEGITEXT000006052581

(11) https://www.archimag.com/vienumerique/2015/10/14/entreprisesaveuglesface-voldonn%C3%A9es

(12) https://www.silicon.fr/cybercrimemadeinfrancerapportthreatmetrix2015 116500.html

(13) https://www.consilium.europa.eu/fr/policies/dataprotectionreform/data-protectionregulation/

NOUS CONTACTER

Infos-client@entreloups.com

06 95 56 38 62

entreloups.com

https://linkedin.com/company/entreloups/

ENTRELOUPS

Dev web & mobile depuis 2007