La sécurité informatique

Elle revêt 3 principaux aspects :

1. Les failles « humaines »
2. Les failles techniques, de programmations
3. Les failles serveurs

Quelle législation s’applique ? Les RGPD selon la CNIL

1. Les failles humaines

A° Quelles sont les principales failles ?

1.1 La connexion d'une clé USB inconnue

La curiosité pousse certaines personnes à connecter à leur ordinateur des clés USB trouvées par hasard, sans en connaître l’origine. Un cybercriminel dispose pourtant de multiples opportunités avec une simple clé USB. Il peut par exemple utiliser un fichier infecté pour accéder à des données et des mots de passe (ingénierie sociale) ou exploiter une faille sans correctif connu et en faire profiter son réseau. Il peut même configurer une clé USB pour que celle-ci se fasse passer auprès de l’ordinateur pour un clavier qui exécute des commandes via des entrées de touches simulées. On appelle ça le HID Spoofing.

1.2 La revente des données de l’entreprise

Toute personne qui a déjà travaillé dans un département R&D sait à quel point les données de l’entreprise ont de la valeur. Vendre des plans, des recettes, des schémas de développement ou autres secrets business à des concurrents peut représenter une affaire en or pour les employés. Un collaborateur mécontent, une impulsion criminelle et une opportunité de transfert de données, des ingrédients suffisants pour entraîner une entreprise dans une situation de crise.

1.3 Voler des données clients lors d'un changement d'employeur

Dans certains secteurs, c'est une pratique courante de prendre des données clients sensibles d'un employeur pour les emmener vers un autre. L'exemple classique est un responsable des ventes embauché chez un concurrent et qui revient peu de temps après vers ses anciens clients pour refaire des affaires. Cela peut paraître anodin, mais il s'agit pourtant bien d'un vol de données, pas moins grave que si l'employé conservait un ordinateur portable et la voiture de l'entreprise à la fin de son contrat de travail.

1.4 Le confort l'emporte sur la sécurité

L'inconvénient d'installer des mises à jour Windows ou Mac, c'est qu'il faut redémarrer l'ordinateur. Quant aux scans anti-virus, ils ont tendance à ralentir la machine. Certains collaborateurs préfèrent donc se passer totalement de tels processus. S'il est possible pour eux de désactiver les mises à jour ou les anti-virus, ils n'hésiteront pas à le faire et la sécurité IT en souffrira grandement !

1.5 La fraude au président

Cette arnaque consiste généralement pour un escroc à se faire passer pour le patron d'une entreprise par téléphone ou email et faire en sorte qu'un employé transfère une grosse somme d'argent vers un pays étranger. Le collaborateur embrouillé par l'autorité de son interlocuteur approuve ainsi la transaction. Cette escroquerie peut causer des dommages de plusieurs millions d'euros avec des conséquences parfois lourdes pour les entreprises touchées et les employés dupés.

1.6 Les téléchargements et streaming non protégés

La plupart des employés ont un accès direct à Internet sur leur lieu de travail. Et malgré l'amélioration constante des systèmes de sécurité IT et des filtres web, certains collaborateurs, pourtant expérimentés et avec une bonne connaissance IT, trouvent tout de même le moyen d'accéder à des contenus à risque. Certains d'entre

eux n’hésitent pas à streamer des films récents le soir sans surveillance ou à télécharger une masse de fichiers douteux, potentiellement malveillants.

1.7 Les incidents de sécurité dissimulés

Dans 40% des entreprises dans le monde, des collaborateurs ont déjà caché sous le tapis des incidents liés à la sécurité IT (sondage Kaspersky/B2B International auprès de 5000 entreprises). Ces incidents de sécurité peuvent être des escroqueries ou des attaques de Malware, ayant entraîné des transferts de programmes malveillants sur l’ordinateur du collaborateur. Si un employé concerné garde le silence à propos de cet incident, le code malveillant peut se propager sur le réseau de l’entreprise.

1.8 Le BYOD (Bring Your Own Devil !)

Quand les collaborateurs apportent leurs propres appareils mobiles dans l’entreprise, c’est le diable qui entre ! Les données sensibles de l’entreprise transitent ainsi sur des smartphones privés, sans pour autant que ceux-ci soient sécurisés. Un smartphone sur lequel des chiffres de ventes récents sont transférés dans l’après-midi peut ainsi être pris en main dans un bar le soir-même pour une séance photos des dernières vacances. Et la perte possible d’un appareil mobile peut être problématique : d’après une étude, plus de la moitié de tous les incidents de sécurité dans les entreprises seraient causés par la perte de tels appareils.

1.9 L’abus de confiance

Beaucoup de cybercriminels savent abuser de la confiance des gens. En entreprise, il est fréquent qu’un administrateur IT appelle l’un de ses collègues au téléphone et lui demande son mot de passe. Soit parce que cela facilite la télémaintenance, soit pour gagner du temps, voire pour éviter de se déplacer. Et généralement, ce collègue lui indique son mot de passe sans sourciller. Et si ce soi-disant administrateur IT avait été un cybercriminel inconnu ? Cet exemple est déclinable de multiples façons.

1.10 La négligence

Les collaborateurs qui ne se sentent pas concernés sont des poisons pour toutes les entreprises. Non seulement ils sont rarement productifs, mais ils représentent également une vulnérabilité potentielle en termes de sécurité IT. Leur attitude « je-m'en-foutiste » peut se refléter dans tout ce qui concerne la sécurité. Qu'il s'agisse de la gestion laxiste des mots de passe, de la divulgation d'informations sensibles à n'importe qui ou encore la distribution trop large de droits d'accès lors de partages de fichiers avec des partenaires externes, la sécurité est constamment compromise avec ce type de collaborateurs.

1.11 Spam et Phishing

La faille la plus classique de la sécurité IT est toujours très populaire ! Il est donc toujours fortement déconseillé d'ouvrir par curiosité les pièces jointes d'emails provenant d'expéditeurs inconnus ou encore d'entrer des informations sensibles dans des champs de saisie suspects. Car ces erreurs continuent de causer des pertes annuelles qui se comptent en milliards pour les entreprises.

1.12 Gardez un œil sur le patron !

Non, le PDG ou chef d'entreprise n'est pas meilleur que les autres en matière de sécurité. Celui ou celle qui dirige l'entreprise doit également figurer dans la liste des éléments à surveiller de près. De nombreux patrons ont en effet le sentiment d'être au-dessus de ce type d'erreurs et rejettent ainsi les logiciels de sécurité en pensant que de telles choses ne peuvent pas leur arriver.

- Faible sécurité du mot de passe
- Manipulation imprudente de données
- Sécurité logicielle inadaptée
- Gestion inefficace de l'accès aux données
- Faible sensibilisation à la sécurité

B° Les bonnes pratiques

1. Un bon mot de passe, selon la CNIL

Un mot de passe doit contenir douze caractères ou plus, voir être composé d'une phrase, qui doit contenir au moins :

· Un nombre
· Une majuscule
· Un signe de ponctuation ou un caractère spécial (dollar, dièse, ...)
· Une douzaine de mots

2. Les mails, selon ANSSI (Agence nationale de la sécurité des systèmes d'information)

2.1 N'ayez pas une confiance aveugle dans le nom de l'expéditeur

Soyez donc attentif à tout indice mettant en doute l'origine réelle du courriel, notamment si le message comporte une pièce jointe ou des liens : incohérence de forme ou de fond entre le message reçu et ceux que votre interlocuteur légitime vous envoie d'habitude, par exemple. En cas de doute, contactez votre interlocuteur pour vérifier qu'il est à l'origine du message.

Et même si l'expéditeur est le bon, il a pu, à son insu, vous envoyer un message infecté.

Vous devez admettre que dans le domaine de la messagerie électronique, il n'existe pas d'expéditeur a priori de confiance.

2.2 Méfiez-vous des pièces jointes

Elles peuvent contenir des virus ou des espiogiciels.

Assurez-vous régulièrement que votre antivirus est activé et à jour.

Si votre poste a un comportement anormal (lenteur, écran blanc sporadique, etc.), faites-le contrôler.

2.3 Ne répondez jamais à une demande d'informations confidentielles

Les demandes d'informations confidentielles, lorsqu'elles sont légitimes, ne sont jamais faites par courriel (mots de passe, code PIN, coordonnées bancaires, *etc*.). En cas de doute, là encore, demandez à votre correspondant légitime de confirmer sa demande car vous pouvez être victime d'une tentative de filoutage, ou phishing. Il s'agit d'une technique utilisée par des personnes malveillantes, usurpant généralement l'identité d'un tiers ou simulant un site dans lesquels vous avez a priori confiance (une banque, un site de commerce, etc.) dans le but d'obtenir des informations confidentielles, puis de s'en servir.

Les messages du type chaîne de lettres, porte-bonheur ou pyramide financière, appel à solidarité, alerte virale, ou autres, peuvent cacher une tentative d'escroquerie. Évitez de les relayer, même si vous connaissez l'expéditeur.

2.4 Passez votre souris au-dessus des liens, faites attention aux caractères accentués dans le texte ainsi qu'à la qualité du français dans le texte ou de la langue pratiquée par votre interlocuteur

En passant la souris au-dessus du lien proposé, vous pouvez repérer s'il pointe bien vers l'adresse du site annoncée dans le message. Si l'adresse est différente, soyez méfiant, et évitez de cliquer sur le lien. De manière générale, il est préférable de saisir manuellement l'adresse dans le navigateur. Dans la plupart des tentatives de filoutage, notamment lorsqu'elles viennent de l'étranger et que le texte a été traduit par un logiciel, l'orthographe et la tournure des phrases sont d'un niveau très moyen, et les caractères accentués peuvent être mal retranscrits. Toutefois, on constate qu'un nombre croissant de tentatives de filoutage emploie un français correct.

Soyez donc le plus vigilant possible lors de la réception de tels messages.

2.5 Paramétrez correctement votre logiciel de messagerie

- mettez à jour vos logiciels, si possible en activant la procédure de mise à jour automatique ;
- paramétrez votre logiciel de messagerie pour désactiver la prévisualisation automatique des courriels ;
- dans les paramètres de sécurité en options, interdisez l'exécution automatique des ActiveX et des plug-ins et les téléchargements, soit en les désactivant, soit en imposant de vous en demander l'autorisation ;
- dans un environnement sensible, lisez tous les messages au format texte brut.

Les particularités du télétravail. Le fait de travailler sur des terminaux non sécurisés favorise les attaques. Il est alors recommandé de mettre en place un réseau privé virtuel ou un VPN pour toutes les données professionnelles. Le réseau privé permet d'échanger des données sécurisées entre le poste de travail à distance et le réseau de l'entreprise.

C° Le télétravail

10 recommandations de sécurité pour les télétravailleurs

Vous êtes confinés et devez avoir recours au télétravail pour maintenir votre activité. Vous ne disposez parfois pas d'équipement professionnel pour télétravailler et devez le faire avec vos moyens informatiques personnels (ordinateur, tablette, téléphone, comptes de messagerie…).

Afin de préserver au mieux la sécurité de votre entreprise, appliquez les 10 recommandations suivantes :

1. **Si vous disposez d'équipements professionnels, séparez vos usages** : Séparez bien vos usages professionnels et personnels au risque de les confondre et de générer des fautes

de sécurité qui pourraient être préjudiciables à votre entreprise. L'activité professionnelle doit se faire sur vos moyens professionnels et seulement sur vos moyens professionnels et l'activité personnelle doit se faire seulement sur vos moyens personnels. En savoir plus.

2. **Appliquez strictement les consignes de sécurité de votre entreprise** : Ces mesures de sécurité visent à protéger votre entreprise, donc votre activité. Si vous rencontrez des difficultés à appliquer les mesures prescrites, remontez l'information et demandez conseil à votre entreprise, mais ne les contournez pas de votre propre chef, car vous n'êtes probablement pas en mesure d'apprécier l'étendue des risques que vous pourriez prendre et faire prendre à votre entreprise

3. **Ne faites pas en télétravail ce que vous ne feriez pas au bureau :** A fortiori sur vos équipements professionnels si vous en disposez. Ayez une utilisation responsable et vigilante de vos équipements et accès professionnels. Si vous utilisez vos moyens personnels en télétravail, ayez conscience que vos activités personnelles peuvent faire prendre un risque aussi à votre entreprise, redoublez donc d'attention et de prudence.

4. **Appliquez les mises à jour de sécurité sur tous vos équipements connectés (PC, tablettes, téléphones…)** : Et ce dès qu'elles vous sont proposées afin de corriger les failles de sécurité qui pourraient être utilisées par des pirates pour s'y introduire et les utiliser pour attaquer le réseau de votre entreprise au travers de vos accès. En savoir plus.

5. **Vérifiez que vous utilisez bien un antivirus et scannez vos équipements** : Vérifiez que tous vos équipements connectés (PC, téléphones, tablettes…) sont bien protégés par un antivirus, qu'il est bien à jour, et effectuez une analyse

complète (scan) de vos matériels. Si un matériel ne peut avoir d'antivirus, évitez le plus possible de l'utiliser pour accéder au réseau de votre entreprise.

6. **Renforcez la sécurité de vos mots de passe** : Utilisez des mots de passe suffisamment longs, complexes et différents sur tous les équipement et services auxquels vous accédez, qu'ils soient personnels ou professionnels. La majorité des attaques est due à des mots de passe trop simples ou réutilisés. Au moindre doute ou même en prévention, changez-les et activez la double authentification chaque fois que cela est possible. En savoir plus.

7. **Sécurisez votre connexion WiFi** : Le télétravail s'opère en général principalement sur votre connexion WiFi personnelle. Il est donc primordial de bien la sécuriser pour éviter toute intrusion sur votre réseau qui pourrait être utilisée pour attaquer votre entreprise. Utilisez un mot de passe suffisamment long et complexe (voir plus haut) et assurez vous que vous utilisez bien le chiffrement de votre connexion en WPA2. Pensez également à mettre à jour régulièrement votre « box Internet » en la redémarrant ou depuis son interface d'administration.

8. **Sauvegardez régulièrement votre travail** : La sauvegarde est le seul moyen permettant de retrouver ses données en cas de cyberattaques, mais également en cas de panne ou de perte de son équipement. Si vous en avez la possibilité, sauvegardez régulièrement votre travail sur le réseau de l'entreprise ou les moyens qu'elle met à disposition à cet effet, mais aussi sur un support externe à votre équipement (clé ou disque USB) que vous débranchez une fois la sauvegarde effectuée. En savoir plus.

9. **Méfiez-vous des messages inattendus** : Que ce soit par messagerie (*email*, SMS, chat…) en cas de message inattendu ou alarmiste, demandez toujours confirmation à l'émetteur par un autre moyen. Il peut s'agir d'une attaque par hameçonnage (*phishing*) visant à vous dérober des informations confidentielles (mots de passe), de l'envoi d'un virus par pièce-jointe ou d'un lien qui vous attirerait sur un site piégé, ou encore d'une tentative d'arnaque aux faux ordres de virement (voir menaces supra).

10. **N'installez vos applications que dans un cadre « officiel » et évitez les sites suspects** : Sur vos équipements professionnels, n'installez de nouvelles applications qu'après l'accord de votre support informatique. Sur vos équipements personnels utilisés en télétravail, n'installez des applications que depuis les sites ou magasins officiels des éditeurs (exemple : Apple App Store,Google Play Store) pour limiter les risques d'installation d'une application piégée pour pirater votre équipement. De même, évitez les sites Internet suspects ou frauduleux (téléchargement, vidéo, streaming illégaux) qui pourraient également piéger vos équipements.

12 recommandations de sécurité liées au télétravail pour les employeurs

Pour faire face à la crise et au confinement imposé par l'épidémie du CORONAVIRUS – COVID-19 les employeurs, entreprises, associations, administrations, collectivités se sont vues devoir mettre en place ou développer dans l'urgence le télétravail pour maintenir, au moins a minima, leurs activités essentielles. L'ouverture vers l'extérieur du système d'information de l'entreprise peut engendrer des risques sérieux de sécurité qui pourraient mettre à mal l'entreprise, voire engager sa survie en cas de cyberattaque.

1. **Définissez et mettez en œuvre une politique d'équipement des télétravailleurs** : Privilégiez autant que possible pour le télétravail l'utilisation de moyens mis à disposition, sécurisés et maîtrisés par l'entreprise. Lorsque ce n'est pas possible, donnez des directives d'utilisation et de sécurisation claires aux employés en ayant conscience que leurs équipements personnels ne pourront jamais avoir un niveau de sécurité vérifiable (voire sont peut être déjà compromis par leur usage personnel).

2. **Maîtrisez vos accès extérieurs** : Limitez l'ouverture de vos accès extérieurs ou distants (RDP) aux seules personnes et services indispensables, et filtrer strictement ces accès sur votre pare-feu. Cloisonnez les systèmes pour lesquels un accès à distance n'est pas nécessaire pour les préserver, surtout s'ils revêtent un caractère sensible pour l'activité de l'entreprise.

3. **Sécurisez vos accès extérieurs** : Systématisez les connexions sécurisées à vos infrastructures par l'emploi d'un « VPN » (*Virtual Private Network* ou « réseau privé virtuel » en français). Outre le chiffrement de vos connexions extérieures, ces dispositifs permettent également de renforcer la sécurité de vos accès distants en les limitant aux seuls équipements authentifiés. La mise en place sur ces connexions VPN d'une double authentification sera également à privilégier pour se prémunir de toute usurpation.

4. **Renforcez votre politique de gestion des mots de passe** : Qu'il s'agisse des mots de passe des utilisateurs en télétravail, mais aussi de ceux en charge du support informatique, les mots de passe doivent être suffisamment longs, complexes et uniques sur chaque équipement ou service utilisé. La majorité des attaques est due à des mots de passe trop simples ou réutilisés. Au moindre doute ou même en prévention, changez-les et activez la double authentification chaque fois

que cela est possible. En savoir plus.

5. **Ayez une politique stricte de déploiement des mises à jour de sécurité** : Et ce, dès qu'elles sont disponibles et sur tous les équipements accessibles de votre système d'information (postes nomades, de bureau, tablettes, smartphones, serveurs, équipements réseaux ou de sécurité…) car les cybercriminels mettent peu de temps à exploiter les failles lorsqu'ils en ont connaissance. Un défaut de mise à jour d'un équipement est souvent la cause d'une intrusion dans le réseau des entreprises. En savoir plus.

6. **Durcissez la sauvegarde de vos données et activités** : Les sauvegardes seront parfois le seul moyen pour l'entreprise de recouvrer ses données suite à une cyberattaque. Les sauvegardes doivent être réalisées et testées régulièrement pour s'assurer qu'elles fonctionnent. Des sauvegardes déconnectées sont souvent indispensables pour faire face à une attaque destructrice par rançongiciel (*ransomware*). En outre, il convient également de s'assurer du niveau de sauvegarde de ses hébergements externes (cloud, site Internet d'entreprise, service de messagerie…) pour s'assurer que le service souscrit est bien en adéquation avec les risques encourus par l'entreprise. En savoir plus.

7. **Utilisez des solutions antivirales professionnelles** : Les solutions antivirales professionnelles permettent de protéger les entreprises de la plupart des attaques virales connues, mais également parfois des messages d'hameçonnage (*phishing*), voire de certains rançongiciels (*ransomware*). Utiliser des solutions différentes pour la protection des infrastructures et pour les terminaux peut s'avérer très complémentaire et donc démultiplier l'efficacité de la protection dans un principe de défense en profondeur.

8. **Mettez en place une journalisation de l'activité de tous vos équipements d'infrastructure** : Ayez une journalisation systématique et d'une durée de rétention suffisamment longue de tous les accès et activités de vos équipements d'infrastructure (serveurs, pare-feu, proxy…), voire des postes de travail. Cette journalisation sera souvent le seul moyen de pouvoir comprendre comment a pu se produire une cyberattaque et donc de pouvoir y remédier, ainsi que d'évaluer l'étendue de l'attaque.

9. **Supervisez l'activité de vos accès externes et systèmes sensibles** : Cette supervision doit vous permettre de pouvoir détecter toute activité anormale qui pourrait être le signe d'une cyberattaque, tels une connexion suspecte d'un utilisateur inconnu, ou d'un utilisateur connu en dehors de ses horaires habituels, ou encore un volume inhabituel de téléchargement d'informations…

10. **Sensibilisez et apportez un soutien réactif à vos collaborateurs en télétravail** : Donnez aux télétravailleurs des consignes claires sur ce qu'ils peuvent faire ou ne pas faire et sensibilisez les aux risques de sécurité liés au télétravail. Cela doit se faire avec pédagogie pour vous assurer de leur adhésion et donc de l'efficacité des consignes. Les utilisateurs sont souvent le premier rempart pour éviter, voire détecter les cyberattaques. Utilisez au besoin nos supports et notre kit de sensibilisation ou encore les recommandations aux télétravailleurs décrites supra. Ces utilisateurs coupés de leur entreprise ont également besoin d'un soutien de qualité et réactif pour éviter toute dérive.

11. **Préparez-vous à affronter une cyberattaque** : L'actualité démontre qu'aucune organisation, quelle que soit sa taille,

n’est à l’abri d’une cyberattaque. Il faut donc admettre que cela n’arrive pas qu’aux autres. La question n’est donc plus de savoir si on va être victime d’une cyberattaque, mais quand on le sera. Il faut donc s’y préparer. L’évaluation des scénarios d’attaques possibles (cf. menaces supra) permet d’anticiper les mesures à prendre pour s’en protéger et de définir également la conduite à tenir pour réagir quand elle surviendra : plans de crise et de communication, contractualisation avec des prestataires spécialisés pour recourir à leur assistance…

12. **Dirigeants : impliquez-vous et montrez l’exemple !** La sécurité est toujours une contrainte qu’il faut accepter à la mesure des enjeux qui peuvent s’avérer vitaux pour les entreprises. L’implication et l’adhésion des dirigeants aux mesures de sécurité est indispensable, tout comme leur comportement qui doit se vouloir exemplaire afin de s’assurer de l’adhésion des collaborateurs.

FAILLES SERVEUR WEB

Ping flood

Le ping flood est une **forme d'attaque** par déni de service. L'attaque provoque donc un « déni de service ». Vous pouvez vous représenter cette attaque comme un canular téléphonique : un hacker malveillant appelle sans cesse et raccroche immédiatement. La liaison est ainsi bloquée et indisponible. Il n'est alors plus possible de répondre aux appels légitimes.

Les attaques de flood connues comme le ping flood, le HTTP flood, SYN Flood et l'UDP Flood consistent à **saturer un système cible avec des demandes insensées** jusqu'à ce qu'il s'écroule. Le ping flood ne doit pas être confondu avec le ping of death qui provoque le crash du système cible sans le surcharger.

Qu'est-ce qu'un ping flood ?

Le ping flood est une cyberattaque visant différents systèmes connectés à Internet. Les systèmes attaqués peuvent être aussi bien des serveurs que des routeurs ou des ordinateurs de particuliers.

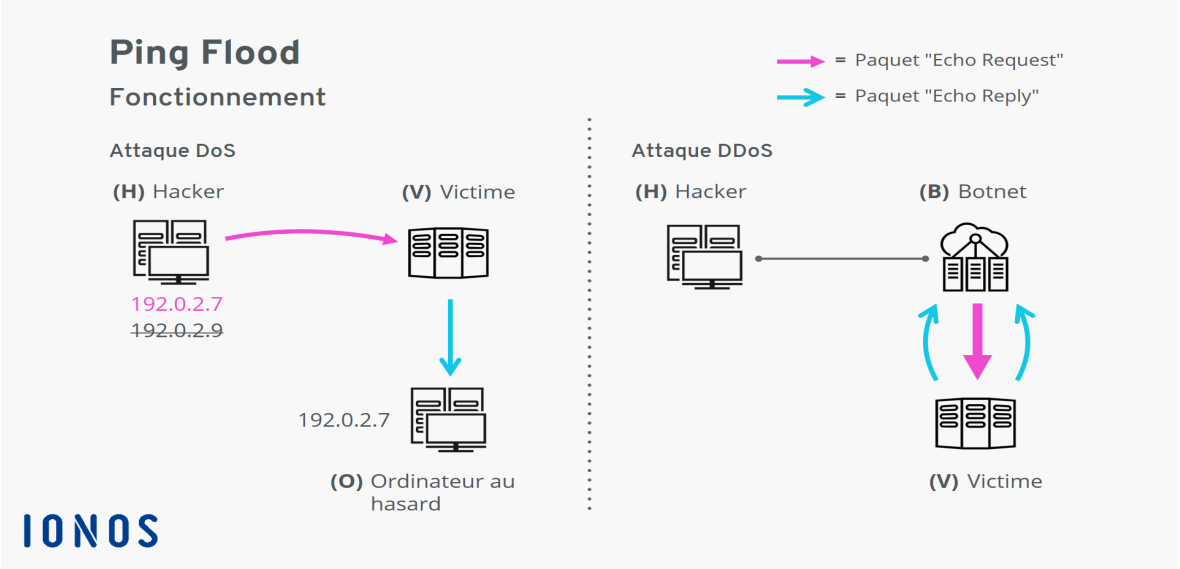
D'un point de vue technique, le ping flood repose sur l'Internet Control Message Protocol (ICMP). Ce protocole et la commande ping correspondante sont normalement utilisés pour réaliser des tests sur le réseau. Un ping flood provoque la **surcharge de l'ordinateur cible avec des paquets « Echo Request » ICPM**. Si le hacker dispose de plus de bande passante que la victime, cette dernière est évacuée du réseau.

Fonctionnement du ping flood

Le fonctionnement du ping flood est simple :

- Le hacker envoie des paquets « Echo Request » par vague à la machine de la victime.
- Cette dernière répond avec des paquets « Echo Reply ».
- Chaque paquet « Echo Request » entrant demande de la bande passante à la victime. Comme un paquet « Echo Reply » est renvoyé pour chaque paquet entrant, le trafic réseau sortant implique un volume de données tout aussi élevé. Si le hacker dispose de suffisamment de bande passante, il peut exploiter toutes les capacités réseau de la victime à disposition. Le trafic réseau légitime est alors interrompu ou s'arrête complètement.

Le ping flood peut être une attaque DoS ou DDoS selon que l'attaque provienne d'un ordinateur individuel ou d'un réseau d'ordinateurs.



Attaque ping flood sous forme de Denial of Service (DoS)

Dans la variante la plus simple de cette attaque, le hacker envoie les paquets « Echo Request » à la victime **depuis une seule machine**. Pour ne pas dévoiler son identité, le hacker usurpe une adresse IP. Un ordinateur au hasard accessible à cette adresse IP sera alors bombardé par les paquets « Echo Reply » correspondants. Cet effet de rétrodiffusion est également appelé « backscatter ». Dans certaines variantes de ping flood, notamment dans les attaques par rebond, la rétrodiffusion est utilisée comme une arme à part entière.

Pour envoyer un ping flood contre sa victime, le hacker utilise la commande ping ou une alternative moderne telle que l'outil hping. **L'attaque commence sur l'invite de commande**. Le ping flood est déclenché à l'aide d'une commande conçue spécifiquement pour l'attaque. Pour des raisons de sécurité, nous ne pouvons présenter ici qu'un modèle approximatif du code hping utilisé :

```
hping --icmp --flood --rand-source -p <Port> <Adresse IP>
```

Jetons un œil aux différentes options :

- L'option *--icmp* indique à l'outil d'utiliser l'ICMP comme protocole.
- L'option *--flood* est tout particulièrement importante ici. Selon la documentation de la commande hping, celle-ci fait en sorte que des paquets soient envoyés aussi rapidement que possible. D'autre part, cette option induit que les paquets « Echo Reply » entrants seront rejetés sans être pris en compte. Par conséquent, au lieu d'envoyer un ping et d'attendre une réponse comme dans une utilisation normale de la commande ping, les pings sont envoyés à répétition aussi rapidement que possible.
- L'option *--rand-source* travestit l'adresse IP de l'expéditeur. Une adresse IP aléatoire est renseignée à la place de la véritable adresse de l'expéditeur.

Attaques ping flood sous forme de Distributed Denial of Service (DDoS)

Pour déclencher un ping flood « distributed », le hacker utilise un botnet. Les bots placés sous le contrôle du hacker lancent un ping flood contre la victime sur ordre du hacker. Comme plusieurs ordinateurs se dressent contre une même cible, la **bande passante disponible du côté du hacker est nettement plus importante**. Seule une cible bien protégée peut résister à ce type d'attaque.

Dans ce scénario, le hacker n'envoie pas les paquets « Echo Request » depuis son ordinateur. Il n'a donc aucune raison de falsifier son adresse IP. Au lieu de cela, les bots agissent depuis leur propre adresse. La rétrodiffusion touche donc sur les ordinateurs zombies du botnet.

Mesure de protection contre les attaques ping flood (ping flood attacks)

Il existe en principe trois méthodes pour se protéger contre les attaques ping flood :

Configurer le système à protéger pour une sécurité élevée

La méthode la plus simple pour se protéger contre les attaques ping flood consiste à **désactiver la fonctionnalité ICMP sur l'appareil de la victime**. Cette mesure offre une solution immédiate lors d'une attaque mais peut également être mise en place de façon préventive pour réduire la fenêtre d'accès.

Par ailleurs, les routeurs et les pare-feu peuvent être configurés de façon à ce que le **trafic réseau malveillant entrant soit identifié et filtré**. L'utilisation de technologies de Load Balancing(en français « répartition de charge ») et de Rate Limiting (« limitation du débit ») contribue à la protection contre les attaques DoS.

Utilisation d’un service basé sur le cloud pour affaiblir les attaques par déni de service

Les grands fournisseurs comme Cloudflare mettent à disposition des serveurs dans des centres de données répartis dans le monde entier. Si vous exploitez votre propre site Internet, vous pouvez faire passer votre trafic de données par ces centres de données. Vous disposerez ainsi d’une **bande passante nettement plus importante** pour absorber les attaques DDoS. D’autre part, le trafic de données est filtré par des systèmes intégrés tels que des pare-feu, des répartiteurs de charge et des limitateurs de débit.

Utilisation d’un matériel spécifique avant le système à protéger

Il est également possible de protéger le système avec un matériel spécifique mais cette solution n’a d’intérêt que pour les entreprises très actives dans le domaine informatique. Ces appareils offrent ou combinent les fonctionnalités de pare-feu, de répartiteurs de charge et de limitateurs de débit et filtrent ou bloquent le trafic réseau malveillant.

HTTP / HTTPS

Qu'est-ce qu'un certificat SSL ?

Un certificat SSL est un fichier de données qui lie une clé cryptographique aux informations d'une organisation. Installé sur un serveur, le certificat active le cadenas et le protocole « https », afin d'assurer une connexion sécurisée entre le serveur web et le navigateur. Le SSL est généralement utilisé pour sécuriser les transactions bancaires, le transfert de données et les informations de connexions. Il est récemment devenu la norme pour sécuriser la navigation sur les sites de réseaux sociaux.

Les certificats SSL lient ensemble :

- Un nom de domaine, un nom de serveur et un nom d'hôte.
- L'identité de l'organisation (nom d'entreprise) et le lieu.

Remarque : A partir d'Août 2020, le cadenas et la barre d'adresse verte utilisés auparavant pour symboliser l'utilisation d'un certificat EV n'apparaîtront plus dans les navigateurs .

L'organisation doit installer le certificat SSL sur son serveur web afin d'initialiser des sessions sécurisées avec les navigateurs. Une fois la connexion sécurisée établie, l'ensemble du trafic entre le serveur et le navigateur sera sécurisé.

Une fois le certificat correctement installé sur le serveur, le protocole HTTP devient HTTPs, le 'S' signifiant 'sécurisé'.

Comment fonctionne un certificat SSL ?

Les certificats SSL utilisent ce qu'on appelle la cryptographie à clé publique.

Ce type de cryptographie exploite la puissance de deux clés qui sont de longues chaînes de nombres générés de manière aléatoire. L'une est appelée clé privée et l'autre clé publique, Une clé publique est connue de votre serveur et disponible dans le domaine public. Elle

peut être utilisée pour chiffrer n'importe quel message. Si Alice envoie un message à Bob, elle le verrouillera avec la clé publique de Bob, mais la seule façon de le décrypter est de le déverrouiller avec la clé privée de Bob. Bob est le seul propriétaire de sa clé privée et il est par conséquent le seul à pouvoir l'utiliser pour déverrouiller le message d'Alice. Si un pirate informatique intercepte le message avant que Bob ne le déverrouille, tout ce qu'il obtiendra est un code cryptographique qu'il ne pourra pas déchiffrer, même avec la puissance d'un ordinateur.

Dans le contexte d’un site web, la communication a lieu entre un site et un serveur. Votre site web et votre serveur sont Alice et Bob.

Pourquoi installer un certificat SSL ?

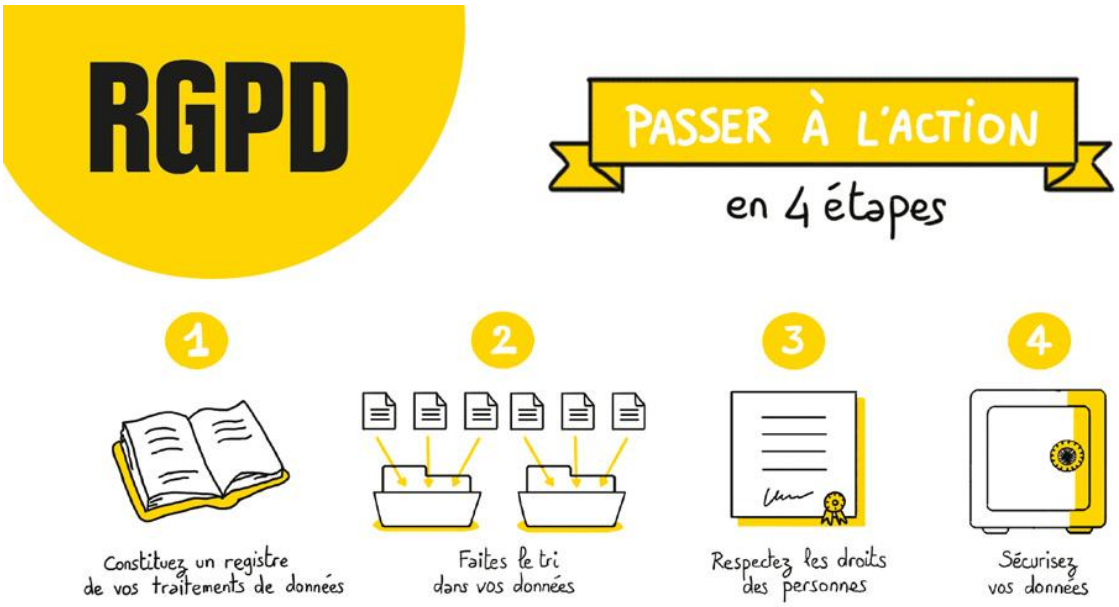
Les certificats SSL protègent vos informations confidentielles telles que les informations relatives aux cartes de crédit, les informations de connexion telles que le nom d'utilisateur, le mot de passe, etc. Ils permettent également :

- Sécuriser les données entre les serveurs
- Améliorer votre classement sur Google
- Renforcer la confiance des clients
- Améliorer les taux de conversion

RGPD
« Règlement Général sur la Protection des Données »

RGPD : par où commencer

Les 4 actions principales à mener entamer et maintenir sa mise en conformité avec les règles de protection des données.



1. **Constituez un registre de vos traitements de données**

En constituant votre registre, vous aurez une vision d'ensemble sur vos traitements de données.

Identifiez les activités principales de votre entreprise qui utilisent des données personnelles.

Exemples : recrutement, gestion de la paye, formation, gestion des badges et des accès, statistiques de ventes, gestion des clients prospects, etc.

Appuyez-vous sur le modèle de registre.

Dans votre registre, créez une fiche pour chaque activité recensée, en précisant :

- **L'objectif poursuivi** (exemple : la fidélisation client) ;
- **Les catégories de données utilisées** (exemple pour la paie : nom, prénom, date de naissance, salaire) ;
- **Qui a accès aux données** (exemple : service chargé du recrutement, service informatique, direction, prestataires, partenaires, hébergeurs) ;
- La durée de conservation de ces données (durée durant laquelle les données sont utiles d'un point de vue opérationnel, et durée de conservation en archive).

Le registre est placé sous la responsabilité du dirigeant de l'entreprise.

Pour avoir un registre exhaustif et à jour, il faut en discuter et être en contact avec toutes les personnes de l'entreprise susceptibles de traiter des données personnelles.

2. Faites le tri dans vos données

Pour chaque fiche de registre créée, vérifiez que :

- les données que vous traitez sont nécessaires à vos activités (par exemple, il n'est pas utile de savoir si vos salariés ont des enfants, si vous n'offrez aucun service ou rémunération attachée à cette caractéristique) ;

- vous ne traitez aucune donnée dite « sensible » ou, si c'est le cas, que vous avez bien le droit de les traiter (voir la fiche « Traitements de données à risque : êtes-vous concerné ? ») ;
- seules les personnes habilitées ont accès aux données dont elles ont besoin ;
- vous ne conservez pas vos données au-delà de ce qui est nécessaire.

À cette occasion, améliorez vos pratiques ! Minimisez la collecte de données, en éliminant toutes les informations inutiles. Redéfinissez qui doit pouvoir accéder à quelles données dans votre entreprise. Définissez, quand cela est possible, des règles automatiques d'effacement ou d'archivage au bout d'une certaine durée dans vos applications.

3. Respectez les droits des personnes

Le RGPD renforce l'obligation d'information et de transparence à l'égard des personnes dont vous traitez les données (clients, collaborateurs, etc.).

Informez les personnes

À chaque fois que vous collectez des données personnelles, **le support utilisé (formulaire, questionnaire, etc.) doit comporter des mentions d'information.**

Vérifiez que l'information comporte les éléments suivants :

- pourquoi vous collectez les données (« la finalité » ; par exemple pour gérer l'achat en ligne du consommateur) ;
- ce qui vous autorise à traiter ces données (le « fondement juridique » : il peut s'agir du consentement de la personne concernée, de l'exécution d'un contrat, du respect d'une obligation légale qui s'impose à vous, de votre « intérêt légitime ») ;
- Qui a accès aux données (indiquez des catégories : les services internes compétents, un prestataire, etc.) ;

- Combien de temps vous les conservez (exemple : « 5 ans après la fin de la relation contractuelle ») ;
- Les modalités selon lesquelles les personnes concernées peuvent exercer leurs droits (via leur espace personnel sur votre site internet, par un message sur une adresse email dédiée, par un courrier postal à un service identifié) ;
- Si vous transférez des données hors de l'UE (précisez le pays et l'encadrement juridique qui maintient le niveau de protection des données).

Appuyez-vous sur les exemples de mentions.

Pour éviter des mentions trop longues au niveau d'un formulaire en ligne, vous pouvez par exemple, donner un premier niveau d'information en fin de formulaire et renvoyer à une **politique de confidentialité / page vie privée** sur votre site internet.

À l'issue de cette étape, vous avez répondu à votre obligation de transparence.

Permettez aux personnes d'exercer facilement leurs droits

Les personnes dont vous traitez les données (clients, collaborateurs, prestataires, etc.) ont des droits sur leurs données : droit d'accès, de rectification, d'opposition, d'effacement, à la portabilité et à la limitation du traitement.

Vous devez leur donner les moyens d'exercer effectivement leurs droits. Si vous disposez d'un site web, prévoyez un formulaire de contact spécifique, un numéro de téléphone ou une adresse de messagerie dédiée. Si vous proposez un compte en ligne, donnez à vos clients la possibilité d'exercer leurs droits à partir de leur compte.

Mettez en place un processus interne permettant de garantir l'identification et le traitement des demandes dans des délais courts (1 mois au maximum).

Bonne pratique : soyez réactifs !

Bien traiter les demandes des consommateurs quant à leurs données personnelles, c'est :

- renforcer la confiance qui sécurise la relation-client ;
- vous mettre à l'abri de critiques sur les réseaux sociaux, ou de plaintes auprès de la CNIL.

À l'issue de cette étape, vous serez en capacité de répondre aux demandes des personnes concernées.

> **Pour en savoir plus** : « Respecter les droits des personnes ».

4. Sécurisez vos données

Si le risque zéro n'existe pas en informatique, vous devez prendre les mesures nécessaires pour sécuriser les données.

Cela vous permet aussi de protéger votre patrimoine de données en réduisant les risques de pertes de données ou de piratage.

Les mesures à prendre, informatiques ou physiques, dépendent de la sensibilité des données que vous traitez et des risques qui pèsent sur les personnes en cas de d'incident.

Des réflexes doivent être mis en place : mettre à jour de vos antivirus et logiciels, bien choisir ses mots de passe, chiffrer vos données dans certaines situations et faire des sauvegardes.

Les failles de sécurité ont également des conséquences pour ceux qui vous ont confié des données personnelles : Ayez à l'esprit les conséquences pour les personnes et pour votre entreprise.

Exemple : vous êtes restaurateur et vous livrez à domicile. Vos clients vous communiquent leur adresse précise et le code d'entrée de leur immeuble. Si ces informations sont piratées ou perdues, elles peuvent être utilisées pour s'introduire frauduleusement au

domicile de votre client. Conséquence désastreuse pour vos clients, mais aussi pour vous !

BONNE PRATIQUE

Pour évaluer le niveau de sécurité des données personnelles dans votre entreprise, voici quelques questions à se poser :

- Les comptes utilisateurs internes et externes sont-ils protégés par des mots de passe d'une complexité suffisante ?
- Les accès aux locaux sont-ils sécurisés ?
- Des profils distincts sont-ils créés selon les besoins des utilisateurs pour accéder aux données ?
- Avez-vous mis en place une procédure de sauvegarde et de récupération des données en cas d'incident ?

Pour en savoir plus :

- Guide des bonnes pratiques de l'informatique réalisé par l'ANSSI et la CPME sur le site internet www.cybermalveillance.gouv.fr
- Guide sécurité des données personnelles de la CNIL

Pour vous aider en cas de difficultés (un sinistre, une attaque informatique, etc.), le site gouvernemental www.cybermalveillance.gouv.fr vous propose de l'aide en ligne ainsi qu'une liste de prestataires approuvés.

BONNE PRATIQUE

L'approche assurantielle au-delà du RGPD :

Cette démarche d'anticipation sur le niveau global de sécurité peut être complétée par une approche assurantielle. Renseignez-vous auprès de ces professionnels sur le contenu possible des polices d'assurance (responsabilité civile, dommages couverts…) et surtout sur les services à l'assuré (notamment l'assistance en cas de sinistre, de gestion de crise…).

Signalez à la CNIL les violations de données personnelles

Votre entreprise a subi une violation de données (des données personnelles ont été, de manière accidentelle ou illicite, détruites, perdues, altérées, divulguées ou vous avez constaté un accès non autorisé à des données) ?

Vous devez **la signaler à la CNIL** dans les 72 heures si cette violation est susceptible de représenter un risque pour les droits et libertés des personnes concernées. Cette notification s'effectue en ligne sur le site web de la CNIL.

Si ces risques sont élevés pour ces personnes, vous devrez les en informer.

À l'issue de cette étape, vous serez en capacité d'assurer une protection des données personnelles en continu et de faire face aux incidents.

FAILLES TECHNIQUES

Les failles de sécurité d'un site ou d'une application web qui dérivent d'une vulnérabilité au niveau du développement informatique de l'application sont appelées des failles techniques. Leurs causes se trouvent soit dans un erreur de programmation, soit dans un manque d'attention aux bonnes pratiques de vérification et de validation des données externes acceptées par l'application.

Injection SQL

Il s'agit d'une vulnérabilité qui concerne les requêtes SQL et les formulaires html souvent utilisés pour récupérer les informations fournies par un utilisateur. En utilisant des caractères spécifiques introduits via ces formulaires, un utilisateur malintentionné peut modifier une requête SQL et provoquer des problèmes dans la base de données vers laquelle se dirige la requête.
Sur la page de connexion d'un site web, par exemple, un utilisateur peut essayer de se connecter même sans avoir les bonnes coordonnées pour le faire. Il peut utiliser un login, un prénom ou un e-mail valide pour le site, mais, au lieu d'envoyer le bon mot de passe pour y accéder, il injecte par le formulaire une chaîne de caractères comme la suivante :

password: 1=1' or pass123.

De cette façon, si la requête SQL qui utilise les données passées par ce formulaire n'est pas suffisamment protégée contre les injections SQL, l'utilisateur pourra se connecter au site en utilisant n'importe quel mot de passe.

Comment pallier les vulnérabilités liées aux injections SQL?

En préparant les requêtes SQL en PHP avec l'instantiation de la classe PDO et l'utilisation de la méthode BindParam. En faisant une *white list* des champs de saisie et en évitant d'afficher des messages d'erreur détaillés, utiles à un attaquant.

Faille XSS

XSS c'est l'acronyme pour l'expression en anglais (cross-site scripting).

Les vulnérabilités XSS ciblent des scripts intégrés dans une page qui sont exécutés côté client, plutôt que côté serveur. Ces failles peuvent survenir lorsque l'application prend des données non fiables et les envoie au navigateur Web sans validation appropriée.

Les attaquants peuvent utiliser XSS pour exécuter des scripts malveillants sur les utilisateurs dans ce cas les navigateurs victimes. Étant donné que le navigateur ne peut pas savoir si le script est fiable ou non, le script sera exécuté et l'attaquant peut détourner les cookies de session, altérer les sites Web ou rediriger l'utilisateur vers des sites Web indésirables et malveillants.

XSS est donc une attaque qui permet à l'attaquant d'exécuter les scripts sur le navigateur de la victime.

Comment pallier les vulnérabilités liées aux failles XSS?

En utilisant la méthode htmlspecialchars de PHP, une méthode qui convertit des caractères spéciaux en entités HTML et bloque ainsi l'insertion d'un script malveillant dans le script originel.

L'attaque par force brute

Une attaque brute force permet de craquer un mot de passe en testant toutes les combinaisons de lettres / chiffres / caractères spéciaux possibles jusqu'à trouver la combinaison parfaite permettant d'accéder par exemple à un compte administrateur d'un site web. Il s'agit de tester plusieurs mots de passe un à un afin de trouver la bonne réponse. Il est souvent combiné à des dictionnaires qui sont des fichiers texte de plusieurs gigaoctet de noms, prénoms, mot du dictionnaire etc… Ils sont généralement composés d'un mot par ligne, où chaque mot sera testé.

Comment pallier les vulnérabilités liées aux attaques par force brute?

– Masquer les pages de connexion à l'administration de votre site web
– Ne pas utiliser de nom d'utilisateur type "admin"
– Limiter les tentatives de connexions en appliquant un bannissement des adresses IP suspectes qui auraient tenté plusieurs connexions échouées.
– Utiliser un anti-bot
– Utiliser des mots de passe complexes

La faille RFI (Remote File Inclusion)

La vulnérabilité RFI que l'on trouve généralement sur les sites internet permet d'inclure un fichier distant, d'exécuter du code sur le serveur, de voler des données etc … Cette vulnérabilité est présente dans tous les langages scripts (PHP, ASP …), le pirate pourra inclure l'url ciblant un fichier malveillant de façon à ce qu'il soit exécuté par le serveur de la victime.

Par exemple :

```
if (isset($_GET['NAME'])) {
    $name= $_GET['NAME'];
}
include($name. '.php');
```

Et voici la vulnérabilité, le fichier à inclure dépend uniquement du contenu de la requête GET qui est donc manipulable directement par l'url, ce qui peut aussi permettre d'en savoir plus sur l'arborescence du serveur.

Comment pallier cette vulnérabilité liée au RFI ?

Éviter l'écriture du nom du fichier php à partir des informations obtenues de la variable globale $_GET. Vérifier que le fichier à charger soit bien parmi ceux qui font partie du projet et qu'il ait l'extension correcte.

https://web.maths.unsw.edu.au/~lafaye/CCM/attaques/attaques-web.htm
https://www.globalsign.com/fr/centre-information-ssl/definition-certificat-ssl
https://www.cnil.fr/fr/rgpd-par-ou-commencer

La vulnérabilité (faille) Upload

Définition

Beaucoup de sites Web offrent la possibilité aux clients d'y uploader des fichiers comme des photos, des vidéos, des CV... Donc il ne s'agit pas vraiment d'une vulnérabilité, mais c'est le fait de ne pas contrôler ce que le client charge sur le serveur qui constitue une vulnérabilité très dangereuse.

Le principe de l'attaque est très simple. Le pirate essaie d'uploader un fichier qui contient du code malveillant ou un code PHP de sa création. Si la faille est là alors le fichier finira pas atterrir sur le serveur. Il suffit ensuite au pirate d'appeler son fichier pour que celui-ci s'exécute.

Bien entendu une telle attaque peut avoir de graves conséquences comme par exemple:

- Espionnage des fichiers et dossiers du site
- Accès au fichiers systèmes et fichiers confidentiels
- Destruction ou altération de données existantes sur le serveur
- Prise de contrôle du serveur

Exploitation

Imaginons que le site Web contient un champ d'upload de fichiers qui permet aux utilisateurs de charger leurs photos de profil. Si la vulnérabilité est là alors le pirate peut créer un document PHP du nom de **crawler.php** qui contient à titre d'exemple le code suivant:

```
$pt = opendir('/');

while($entree = readdir($pt)){

   echo $entree;

}

closedir($pt);
```

Si le pirate réussit à charger ce fichier PHP sur le serveur, alors il pourra ensuite l'appeler via le navigateur en utilisant son URL comme ceci par exemple:

```
http://www.site-victime.php/crawler.php
```

Comme vous l'avez deviné, le fichier chargé va lister tous les fichiers et dossiers à la racine du site Web, ce qui n'est pas tellement dangereux. Mais le pirate aurait pu écrire un code PHP plus dévastateur.

Comment s'en protéger?

Au niveau du code PHP

Comme d'habitude, la vulnérabilité est due au mauvais contrôle des entrées de l'utilisateur, alors qu'il suffisait de vérifier si le type/Mime du fichier uploadé correspond bien à une image JPEG ou PNG en utilisant le code suivant par exemple:

```
<?php

if(preg_match("#jpeg|png#",$_FILES["photo"]["type"]))

// Accepter l'upload

else

echo "Format du fichier invalide.";

?>
```

Il faut également penser à isoler les fichiers chargés dans un dossier à part pour minimiser les risques de rebond au cas où il s'agit d'un fichier malveillant. Renommer les fichiers chargés sera aussi d'une grande utilité car le pirate aura du mal à appeler son fichier s'il ne connaît pas son chemin et son nom.

Une bonne pratique consiste à changer les droits du fichier chargé à l'aide de la fonction **chmod()**.