

REMY RAYNIER
AXEL IBANEZ
BTS SIO

Dossier Cybercriminalité



1. Tableau des attaques

type	fonction	objectif	vos rêves
Usurpation d'identité	<p>Le piratage de compte désigne la prise de contrôle par un individu malveillant d'un compte au détriment de son propriétaire légitime. Il peut s'agir de comptes ou d'applications de messagerie, d'un réseau social, de sites administratifs, de plateformes de commerce en ligne.</p> <p>En pratique, les attaquants ont pu avoir accès à votre compte de plusieurs manières : le mot de passe était peut-être trop simple, vous avez précédemment été victime d'hameçonnage (<i>phishing</i> en anglais) où vous avez communiqué votre mot de passe sans le savoir, ou bien vous avez utilisé le même sur plusieurs sites dont l'un a été piraté.</p>	<p>Dérober des informations personnelles, professionnelles et/ou bancaires pour en faire un usage frauduleux (revente des données, usurpation d'identité, transactions frauduleuses, spam, etc.).</p>	<p>Pour palier à ce problème il faut des mots de passe, une demande régulière de ce connecter un système de double authentification</p>
Spam	<p>Le spam électronique, également appelé courrier indésirable ou pourriel, désigne une communication électronique non sollicitée à des fins publicitaires, commerciales ou malveillantes. Dans la majorité des cas, il s'agit de messages de prospection commerciale ne respectant</p>	<ul style="list-style-type: none">– Vente de produits ou de services, publicité virale, propagande, etc.– Diffusion de virus,– Vol de données personnelles et/ou professionnelles,– Escroquerie à caractère financier.	<p>Soyez vigilant lorsque vous communiquez votre adresse de messagerie.</p> <p>Ne répondez pas aux dont vous ne connaissez pas l'expéditeur.</p> <p>Ne pas ouvrir les</p>

	<p>pas les obligations légales en matière de consentement des destinataires, mais il peut également revêtir un caractère malveillant : astuces pour gagner de l'argent, sollicitation pour transférer des fonds ou encore tentatives d'hameçonnage (<i>phishing</i> en anglais).</p> <p>Les expéditeurs de spams ciblent essentiellement les comptes de messagerie, mais peuvent aussi utiliser les messageries instantanées ou les réseaux sociaux. Un spam électronique peut parfois même contenir un logiciel malveillant (un rançongiciel par exemple) qui pourrait permettre d'utiliser ou de bloquer votre appareil à votre insu.</p>		<p>pièces jointes ou lien pas connus.</p> <p>Utiliser des logiciel anti-spam pour limiter les spam.</p> <p>Soyez vigilant lorsque vous répondez à des formulaires d'inscription, des bons de commande ou quand vous participez à des jeux-concours.</p> <p>Désabonnez-vous ou supprimez les comptes (services, applications, sites Internet) que vous n'utilisez plus.</p> <p>Créez des règles dans votre boîte de messagerie.</p> <p>Créez différentes adresses de messagerie ou des « alias » en fonction de vos besoins.</p>
Vol	Prendre, s'approprier quelque chose qui est le bien d'autrui par la ruse ou par la force	L'objectif du vol est de voler pour revendre ou faire du chantage	Pour pallier ce problème, toute les appareils contenant des information de l'entreprise doivent rester dans l'entreprise ou être

			protégé par des mot de passe et il ne doit pas contenir d'information dans le disque.
Hameçonnage	L'hameçonnage (<i>phishing</i> en anglais) est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe...) et/ou bancaires en se faisant passer pour un tiers de confiance. Il peut s'agir d'un faux message, SMS ou appel téléphonique de banque, de réseau social, d'opérateur de téléphonie, de fournisseur d'énergie, de site de commerce en ligne, d'administrations, etc.	Voler des informations personnelles ou professionnelles (comptes, mots de passe, données bancaires...) pour en faire un usage frauduleux.	<p>Ne communiquez jamais d'informations sensibles par messagerie ou téléphone.</p> <p>Avant de cliquer sur un lien douteux, positionnez le curseur de votre souris sur ce lien.</p> <p>Vérifiez l'adresse du site qui s'affiche dans votre navigateur.</p> <p>En cas de doute, contactez si possible directement l'organisme concerné.</p> <p>Changer de mots de passe pour les différentes applications.</p> <p>Si le site le permet, vérifiez la date et l'heure de dernière connexion à votre compte.</p>

			Activer la double authentification.
Rançongiciels	<p>Les rançongiciels (<i>ransomwares</i> en anglais) sont des logiciels malveillants qui bloquent l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclament à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès. La machine peut être infectée après l'ouverture d'une pièce jointe, ou après avoir cliqué sur un lien malveillant reçu dans des courriels, ou parfois simplement en naviguant sur des sites compromis, ou encore suite à une intrusion sur le système. Dans la majorité des cas, les cybercriminels exploitent des vulnérabilités connues dans les logiciels, mais dont les correctifs n'ont pas été mis à jour par les victimes.</p>	<p>Extorquer de l'argent à la victime en échange de la promesse (pas toujours tenue) de retrouver l'accès aux données corrompues. Certaines attaques visent parfois simplement à endommager le système de la victime pour lui faire subir des pertes d'exploitation et porter atteinte à son image.</p>	<p>Sauvegarder les données</p> <p>Maintenir à jour les logiciels et systèmes</p> <p>Utiliser et maintenir à jour les logiciels antivirus</p> <p>Cloisonner le système d'information</p> <p>Limiter les droits des utilisateurs et autorisations des applications</p> <p>Maîtriser les accès Internet</p> <p>Mettre en œuvre une supervision des journaux</p> <p>Sensibiliser les collaborateurs</p> <p>Évaluer l'opportunité de souscrire à une assurance cyber</p> <p>Mettre en œuvre un plan de réponse aux cyberattaques</p> <p>Penser sa stratégie</p>

			de communication de crise cyber
DDOS	<p>Une attaque en déni de service ou en déni de service distribué (DDoS pour Distributed Denial of Service en anglais) vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé du service. Ce type d'attaque peut être d'une grande gravité pour l'organisation qui en est victime. Durant l'attaque, le site ou service n'est plus utilisable, au moins temporairement, ou difficilement, ce qui peut entraîner des pertes directes de revenus pour les sites marchands et des pertes de productivité. L'attaque est souvent visible publiquement, voire médiatiquement, et laisse à penser que l'attaquant aurait pu prendre le contrôle du serveur, donc potentiellement accéder à toutes ses données, y compris les plus sensibles (données personnelles, bancaires, commerciales...) : ce qui porte directement atteinte à l'image et donc la crédibilité du propriétaire du site auprès de ses utilisateurs, clients, usagers, partenaires, actionnaires...</p>	<p>Rendre un service indisponible. Le cybercriminel agit pour des motivations politiques, idéologiques, par goût du challenge, chantage, vengeance, ou pour des raisons économiques (concurrence). Cette attaque peut être utilisée pour faire diversion d'une autre attaque visant à voler des données sensibles de sa cible.</p>	<p>interdire le protocole icmp</p> <p>mettre en place des équipement de pare feux anti ddos</p> <p>mettre en place des protocole de filtrage géographique, filtrage des paquets</p> <p>limitation de requête de demande ressource</p> <p>mettre un place un détecteur d'attaque</p>

2. Les précautions à prendre sont :

- Toujours faire attention au lien, fichier, pièce jointe qui vient de l'extérieur de l'entreprise et bien faire attention à celui qui envoie les fichiers.
- Mettre du filtrage ip, de géolocalisation, interdiction de certains protocoles réseaux.
- Mettre en place des pare-feu et des antivirus à jour.
- Mettre en place d'un système d'identification avec mot de passe et pseudonyme.
- Mettre en place un détecteur d'attaque.
- Mettre en place des sauvegardes régulières.

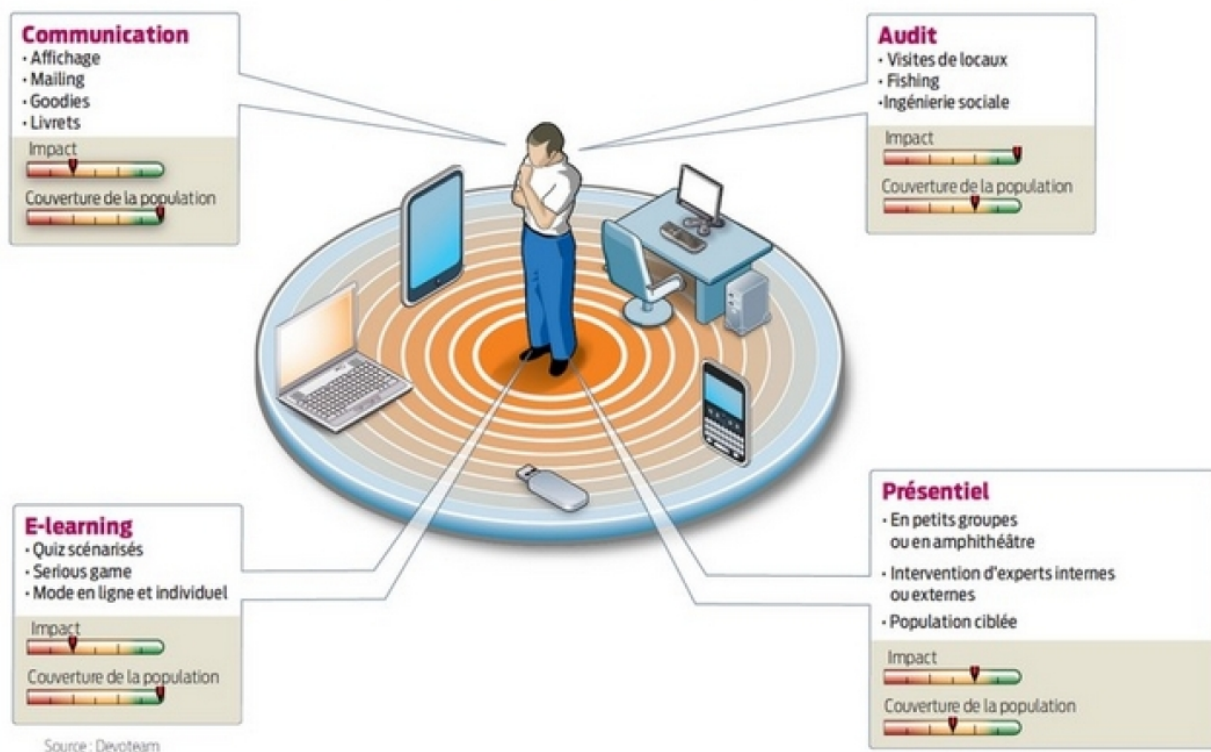
SAUVEGARDES REGULIERES



3. Formations des employés

Les employés pourraient faire une formation (Mooc) et aussi des stages avec les admin réseaux qui leur explique la cybersécurité, et aussi visiter le site du CNIL. Un rendez-vous avec un technicien, un expert, et les tenir toujours informés des nouveautés en termes de cybersécurité et aussi toujours les mettre au courant des dernières menaces. Faire une simulation (un entraînement sur un jeu).

QUATRE MÉTHODES POUR SENSIBILISER LES COLLABORATEURS À LA SÉCURITÉ



4. Le règlement RGPD

Le règlement **oblige** les entreprises à dire ce qu'elles font avec les données de leurs utilisateurs. Il doit dire à l'utilisateur qu'ils prennent leurs données. Il doit montrer que leurs serveurs sont bien protégés et l'intérêt de la prise de données. La désignation d'un délégué à la protection des données. Cartographier **vos** traitements de données personnelles. Organiser les processus internes.

5. Les nouveaux types de risques

On peut prendre pour exemple les dernières vagues de piratages (surtout dans les entreprises qui ont d'énorme base de données sur les clients) et aussi de ransomware ('i wannacry' qui a paralysé une bonne partie des entreprises française). et il faut faire attention que les messages, mail et autres soient bien la bonne personne.


La CNIL peut donner une amende jusqu'à **20 millions d'euros ou 4% du chiffre d'affaires** d'amende en cas de non conformité au RGPD.

6. Synthèse

Pour les entreprises, les nouveaux logiciels malveillants sont les rançongiciels très actifs récemment, un rançongiciel crypte toutes les données de l'entreprise et menace de tout supprimer si on ne paye pas une rançon payable généralement en bitcoins .

Il faut attribuer un chef de la sécurité informatique pour rester vigilant et toujours respecter les règles de sécurité.

En France, 8 entreprises sur 10 sont touchées par des cyber attaques chaque année. Il faut limiter les erreurs humaines, faire attention car 52% des attaques viennent de l'intérieur . Nouvelles attaques surtout des ransomware et piratages. Faire des formations avec les fichiers et documents de la CNIL (LE MOOC) et formation avec l'admin réseau et réunion régulière pour des rappels et les futurs risques.



7.Blockchain

Blockchain est une technologie qui permet de sécuriser et garder la trace d'un ensemble de transactions financières cependant ces transactions sont anonymes, de manière décentralisée, sécurisée et transparente, sous forme d'une chaîne de blocs.

Il faut choisir un bon protocole de consensus car elle permet de valider et sécuriser les contenu des blocs.

Il y a 2 blockchain different privée et publique .La blockchain privée tourne sur un réseau privé sur lequel le gérant peut modifier le protocole quand il le souhaite.et la blockchaine publique est souvent utilisés dans la cryptomonnaie (bitcoin, ethereum, litecoin) on peut donc les choisirent. C'est une monnaie informatique qui fonctionne en (bloc) par exemple les bitcoin sont limités à 21 million de bitcoin. Plus on met de la puissance de calcul, plus on "mine" de la cryptomonnaie, ces calculs permettent de sécuriser le réseau. plus on s'approche des 21 millions, plus c'est dur à miner. certaine autre monnais sont presque identique mais par exemple le litecoin est un script

et oui je pense que sa va remplacer les tiers de confiance car c'est un système ultra sécurisé CEPENDANT une grosse formation nationale des commerce ou autre devra se faire pour expliquer et rendre pret tout les services de blockchain et cryptomonnaie et commerce de france. (je parle d'expérience personnelle).

