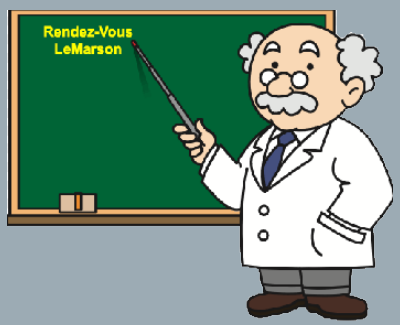
EN DIRECT AVEC LEMARSON

Libérez le RSSI/CISO

Émission animée
par Claude Marson

Le sommaire aujourd'hui
Libérez le RSSI/CISO

- Il faut savoir ce que l'on veut et investir de manière à protéger les usagers, les infrastructures… et les investissements
- A qui avons-nous affaire : toujours comprendre qui est l'ennemi
- Quelle est l'organisation à mettre en face
- Quels profils retenir, celui du ou des techniciens réseaux
- Libérer les techniciens des contraintes de l'entreprise, il faut pratiquer les mêmes organisations et exploiter les mêmes outils, surtout ceux qui sont interdits
- Privilégier le hacking éthique



Libérez le RSSI/CISO

A qui avons-nous à faire ?

- La première génération a débuté avec le premier virus « Brain » de Basit et Amjad Alvi
- La deuxième génération est celle de la recherche du profit
- La troisième génération est celle des organisations criminelles, mafias…
- La quatrième génération (actuelle) est celle de l'économie cybercriminelle, un véritable marché qui s'est constitué pour proposer des services
- La cinquième génération est celle de la cyberguerre entre les états

EN DIRECT AVEC LEMARSON

Libérez le RSSI/CISO

A qui avons-nous à faire ?

Jeux et humour, jeunes et moins jeunes…

- « script kiddies » : jeunes gens capables d'écrire des bouts de scripts et de profiter des faiblesses béantes du TI
- Motivation : s'attaquer au monde des adultes, dont ils pouvaient se sentir exclus. Sans intérêt financier, au-delà d'un complément d'argent de poche indument gagné.
- Les « script kiddies » ont pris de l'âge et se sont généralement assagis.
- Certains d'entre eux ont conservé le goût de l'interdit, d'autant plus savoureux qu'il est quasiment sans risque.
- Ces « old kiddies » ont un égo surdimensionné, convaincus de dominer les technologies informatiques et d'être invulnérables. C'est souvent par ce biais qu'ils se font prendre.
- Certains réussissent quand même à s'en sortir et réussissent relativement bien : Steve Jobs et Steve Wozniak !
- Wozniak (« Berkeley Blue ») et Jobs (« Oaf Tobar ») avaient construit un dispositif de pénétration des systèmes téléphoniques, baptisé « Blue Box », un générateur d'impulsions électroniques (« phreaker ») pour effectuer des appels longue distance
- Wozniak s'est permis d'appeler de cette manière le Vatican, de demander le Pape et de se faire passer pour Henry Kissinger…

Libérez le RSSI/CISO

A qui avons-nous à faire ?

- De très nombreux hackers sont dans la même famille : le célèbre **Kevin Mitnick**, pénétré le système téléphonique de Pacific Bell, alors qu'il était en liberté conditionnelle, justement pour faits de « hacking »…
- **Adrian Lamo**, autiste brillant, avait modifié un article de Reuters, en glissant une « fake new » qu'il avait attribuée à l' « Atorney General » John Ashcroft.
- **Kevin Poulsen** à 24 ans était entré dans le TI d'une radio de Los Angeles, à l'occasion de l'un de ses concours, pour s'approprier une Porsche, un séjour de vacances et 20 000 $... mais aussi 5 ans de prison
- et surtout **Gary McKinnon** qui avait pénétré 97 ordinateurs appartenant aux principales agences américaines et à la NASA, simplement pour y placer des fichiers vides et récupérer quelques informations secrètes.

EN DIRECT AVEC LEMARSON

Libérez le RSSI/CISO

A qui avons-nous à faire ?

La pouponnière du hacking

- Tranche d'âge qui va de 5 à 12 ans.
- **Paul Reuben** est l'un de ces très jeunes enfants, qui a 10 ans a montré comment, en quelques minutes, on pouvait voler les données, messages et contacts, d'un téléphone Android.
- **Betsy Davis**, à 7 ans, n'a eu besoin que d'un simple tutoriel pour hacker un réseau Wi-Fi public, dont elle a mis en évidence les faiblesses.
- **Kristoffer Von Hassel** est le plus étonnant.
- **CyFi**, pseudonyme derrière lequel se cache une jeune personne de 10 ans, connue pour ses capacités à modifier le scénario du jeu en ligne FarmVille, etc.

Libérez le RSSI/CISO

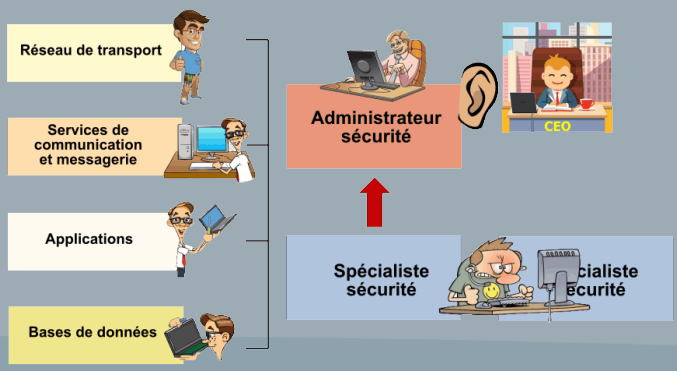
A qui avons-nous à faire ?

- Criminels en col blanc, qui « font de l'argent » avec tout ce qui peut être volé : demandes de rançons, vol de données
- Mafias et organisations structurées
- Ce sont les « mouches du crime » et elles ont seulement changé de coche pendant la dernière décennie.
- Les terroristes : les plus redoutables, car les plus motivés.
- Pour des questions politiques ou religieuses, ils s'estiment en guerre et exploitent les techniques de pénétration et d'attaques pour déstabiliser ou détruire leurs cibles.
- Organisations très compétentes, capables de mettre en œuvre des schémas de pénétration sur plusieurs années.
- Nombreux groupes de ce type : l' « Unified Cyber Caliphate », bras armé de Daesh (état islamique) spécialisé dans les attaques informatiques ou l'Institut Mabna, lié au gouvernement des mollah iraniens, qui a fait de nombreuses victimes, parmi lesquelles cinq agences fédérales, onze sociétés privées étrangères et 144 universités américaines.
- Leurs motivations sont claires, « pures » et « loyales » de leur point de vue, tout comme un saboteur pendant un conflit peut être considéré comme un héros ou un terroriste, selon le camp dans lequel on se trouve.
- Il existe de véritables écoles pour former les membres de ces organisations, qu'il ne faut surtout pas sous-estimer, tant le niveau des enseignants peut être élevé, en analyse numérique, technologies de chiffrement, intelligence artificielle, etc.
- Famille des espions. des hommes et femmes de l'ombre, formés au vol d'informations confidentielles, politiques mais surtout économiques et à la diffusion de fausses informations.
- L'exemple des élections américaines et le rôle joué par Cambridge Analytica, fondé par Steve Bannon et Robert Mercer, est un bon exemple de déstabilisation, venu cette-fois de l'intérieur

Libérez le RSSI/CISO

L'organisation de l'équipe sécurité

- Le RSSI/CISO est une fonction générique qui concerne plusieurs personnes
- La sécurité est essentielle et son responsable doit siéger au Comité Exécutif de l'entreprise
- Ce n'est pas une fonction mineure et sauf pour les PME, ne peut être sous-traitée
- L'organisation dépend de la taille de l'entreprise
- Trois possibilités :
  - Équipe complète dirigée par un gestionnaire de la sécurité, un administratif qui a l'oreille du management
  - Un spécialiste interne (PME, PMI), exclusivement technique à qui on demande de connaître le contexte
  - Surveillance sous-traitée à des prestataires spécialisés
- La sécurité n'est pas une fonction que l'on confie à un préretraité, pour les six mois qui précèdent son départ
- Fonction essentiellement technique qui nécessite des connaissances dans de nombreux domaines, du type ingénieur système, tel qu'il était pratiqué dans les années 90/2000
- Il faut motiver les candidats par des perspectives d'évolution, voire salariales
- …et savoir le sortir des contraintes courantes de l'entreprise : horaires libres, formation continue, pas d'obligation à participation aux réunions inutiles… c'est un électron libre



Libérez le RSSI/CISO

Le rôle du manager

- Fonction de premier plan
- Course contre la montre : il doit être constamment sur le "qui-vive"
- Évaluer et prioriser les ressources à protéger
  - Il connaît le fonctionnement de chaque département.
  - Quels sont les plus gros risques ? Où faut-il faire porter les efforts en priorité.
  - Responsable de la mise en œuvre des plans de reprise (relève), PCA/PRA
- Informer la direction sur les risques, aussi bien internes que pour les clients
  - C'est elle qui sera impactée en cas de problèmes
  - Mettre en évidence les vulnérabilités de l'entreprise…même si ça ne fait pas plaisir…
  - S'exprimer clairement…
  - Intégrer les problématiques nouvelles liées aux données RGPD
  - Suivre le contexte AHA : Autorisations, Habilitations, Accès et s'assurer que les bonnes pratiques sont appliquées dans l'entreprise
- S''appuyer sur une équipe techniquement de haut niveau, c'est lui qui détermine les moyens humains et les compétences… avec la RH
- Rendre compte régulièrement
- Elaborer la charte de sécurité et organiser le prosélytisme sur elle, assure la communication avec le reste de l'entreprise
- Mettre en place les moyens pour calculer les KPI, témoins de l'état sécuritaire de l'entreprise
- Essayer de modéliser la sécurité de l'entreprise, comme s'il s'agissait d'une infrastructure industrielle et mettre en évidence les points sensibles : IoT, mobiles, serveurs publics, DMZ, proxy, reverse proxy, etc
- Anticiper et réagir aux incidents : documenter soigneusement les protocoles d'intervention sur incident
- Acquérir une compétence technique suffisante pour communiquer avec son équipe
- Doit être curieux de ce qui se passe dans le monde des TI
- Faire de la paranoïa une qualité et ne pas se demander si l'entreprise va être attaquée, mais quand…

EN DIRECT AVEC LEMARSON

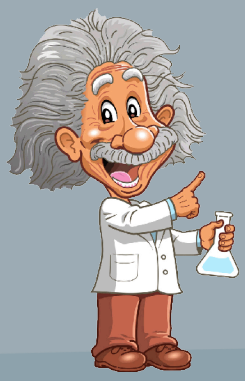
Libérez le RSSI/CISO

Le technicien sécurité

- Personnage à part
- C'est un hacker honnête
- Sa fonction est exclusivement technique
- Il faut le libérer des contraintes de l'entreprise : dans son métier tout se passe dans les forums, certains dans le dark web et pas pendant les "heures de bureau"
- Participe à des organisations "douteuses"
- Exploite les outils interdits et l'entreprise doit lui donner les moyens de les utiliser sans nuire aux ressources qu'il est censé protéger
- Il est allergique à la rigidité de l'entreprise, c'est un contestataire, souvetn en butte avec sa hiérarchie, qu'il accuse de ne rien comprendre…
- Très curieux
- Oublie de venir au bureau parce qu'il a passé la nuit sur un plugin dangereux ou un script malveillant : inutile de le faire pointer, il dort…
- Il n'a pas d'âge et les diplômes n'ont aucune importance
- Il doit se former par des certifications pointues
- La RH doit trouver un moyen d'intégrer ce profil atypique

Libérez le RSSI/CISO

Le profil du technicien sécurité



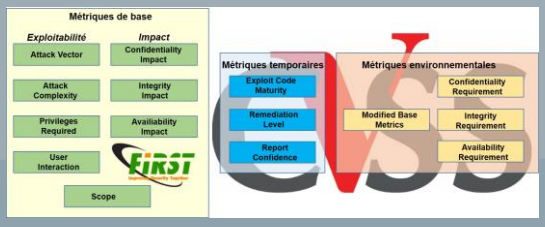
- Programmeur C, assembleur
- Très bonnes connaissances sur les architectures applicatives et les API (Java, script, .NET…)
- Familier des protocoles mis en œuvre à la fois dans les réseaux internes : IP, TCP, UDP, CMIP… et opérateurs : Wi-Fi, Internet, cellulaire
- Bonnes connaissances sur les protocoles propriétaires dans les réseaux
- Bonnes connaissances en architectures machines et outils système : virtualisation, containers…
- Pertinent sur les outils de communication et de coopération : messagerie, IM, Office 365, Gsuite
- Compétent dans les domaines de la cryptologie (chiffrement) et garantie d'intégrité
- Mentalité du hacker : rien ne doit lui résister… et sa satisfaction est souvent purement intellectuelle
- Profil ressemblant à celui d'un homme (femme) système… tombé en désuétude
- … difficile à trouver

EN DIRECT AVEC LEMARSON

Libérez le RSSI/CISO

Les tâches essentielles

- Contact permanent avec l'administrateur de la sécurité
- S'informer des évolutions du TI interne
- Participer aux grands projets structurants
  - Ex d'un projet agile : traite certaines histoires techniques considérées comme prioritaires
- Veille technologique permanente
  - Surveiller la publication des vulnérabilités (CVSS 3.0)
- Veille à ce que techniquement les infrastructures soient à jour : antimalware, VPN, versions d'applications sensibles
- Faire attention à ne pas se laisser distancer

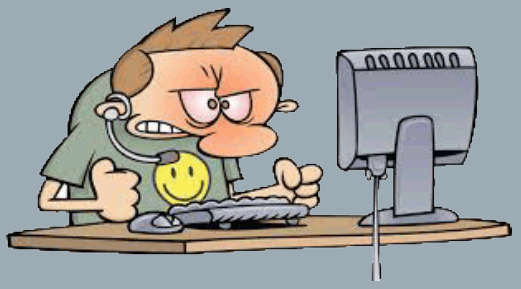


La norme CVSS : 3 familles de métriques, base, temporaires et environnementales. Qui évaluent les failles, selon des formules de calcul standardisées. Les métriques de base sont valorisées par une donnée numérique et les métriques temporaires et environnementales, sont utilisées pour les pondérer.

Libérez le RSSI/CISO

Mesurer la pertinence du RSSI/CISO

- Une tâche importante
- Ce n'est pas Big Brother, simplement s'assurer que l'on va dans la bonne direction
- KPI peu nombreux, quatre au maximum
- Exemples
  - Nombre d'heures d'indisponibilités machines liées à un problème de sécurité, ramené au nombre d'heures total
  - Temps de détection moyen des alertes
  - Temps moyen d'intervention
  - Nombre d'insultes reçues au centre d'appel, en lien avec la sécurité
- Il faut communiquer régulièrement sur ces KPI et ne pas les… trafiquer : l'objectif n'est pas de montrer que tout va bien, mais de quantifier l'évolution de la sécurité TI



Libérez le RSSI/CISO

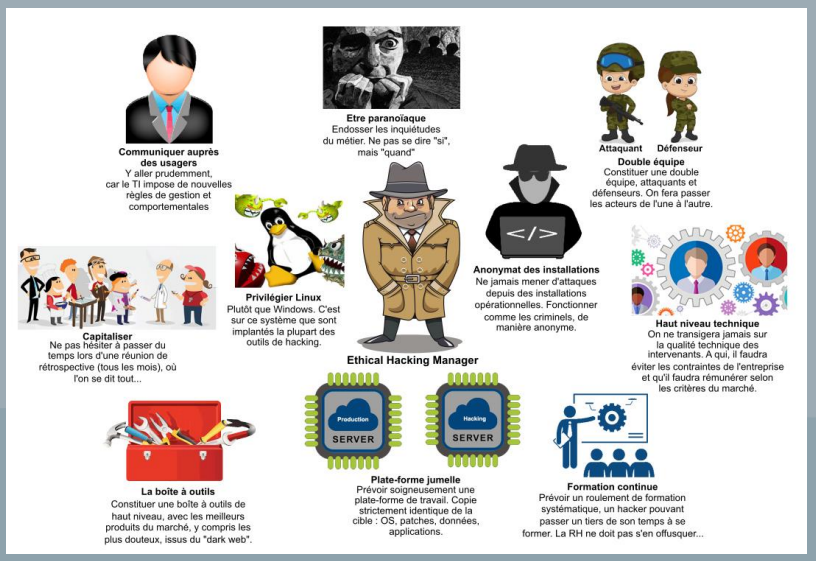
Pratiquer les mêmes techniques que les adversaires

- Il faut les apprendre…
- Participer à des groupes de hacking… sous un faux nom
- Se mettre "dans la peau" d'un criminel, comprendre ses motivations…
- Se faire aider par des consultants sûrs : tests de pénétration réguliers
- Faire appliquer les bonnes pratiques de programmation
- Tester au plus près de la vraie grandeur les scénarii d'attaques

Libérez le RSSI/CISO

La grande question du hacking éthique

- Ne jamais mener d'attaques, depuis une machine interne. Même en simulation.
- Tester nos scénarios sur des sites proches de la production. qui pourra aussi servir de reprise dans le cadre d'un PCA/PRA.
- Communiquer auprès des usagers.
- L'équipe de hacking est bicéphale, avec ceux qui attaquent et ceux qui défendent.
- Une bonne pratique pourra consister, à effectuer à fréquences régulières une réunion de rétrospective, pendant laquelle on se dira tout, surtout ce qui n'aura pas bien fonctionné : retards de compréhension, faiblesses techniques, manque de cohérence dans les actions…
- On veillera à maintenir le contact avec la RH

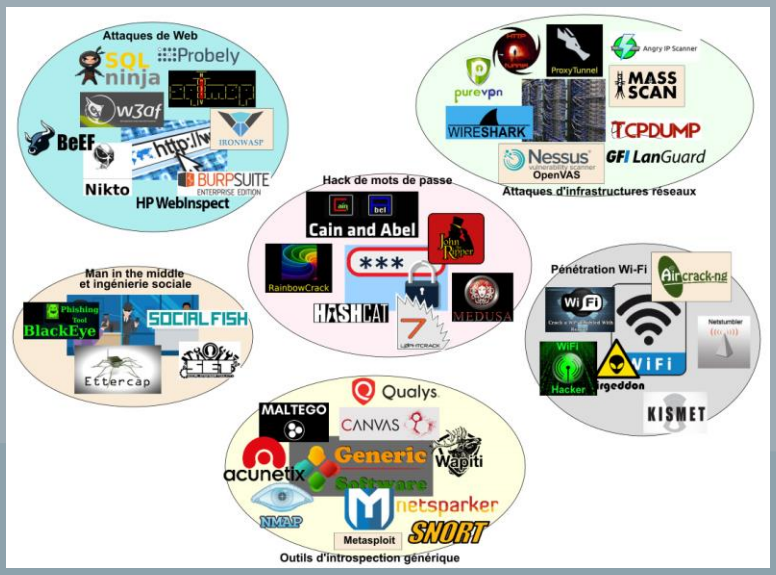


EN DIRECT AVEC LEMARSON

Libérez le RSSI/CISO

Une boîte à outils à votre disposition
Attention…c'est dangereux

- **Aircrack-ng**
- Retrouver les clés utilisées dans les réseaux Wi-Fi, jusqu'au mode de protection WPA-2. De manière à les pénétrer sans autorisation.
- **TCH Hydra**
- L'horreur absolue. S'attaque aux « credentials » d'authentification de plus de 50 protocoles, parmi lesquels les mécanismes Cisco, FTP, FTP, HTTPS, IMAP, IRC, LDAP, MYSQL, NNTP…
- **John the Ripper**
- Pour mener des attaques par force brute, grâce à toute la panoplie des outils et techniques, connus à ce jour. Retrouver les mots de passe (entre autres)
- **Nmap (Network Mapper)**
- Nmap, utilitaire très connu, peut vous aider à faire tomber les protections d'un réseau, mais peut aussi constituer un excellent outil de maintenance.



Nos prochains rendez-vous

Vendredi 31 janvier 2020 :	**Les réseaux neuronaux convolutifs**
Lundi 3 février 2020 :	**Actualités du TI**
Vendredi 7 février 2020 :	**La programmation fonctionnelle**
Vendredi 14 février 2020 :	**La fin du scandale des certificats payants ?**
Vendredi 21 février 2020 :	**La justification financière des projets qualité des données**
Vendredi 28 février 2020 :	**ITIL v4, vous avez du temps à perdre ?**

Je vous remercie de votre attention et à bientôt