Atelier Expression directe

Cybersécurité

CNRA
Confédération Nationale des Radios Associatives

Intervenants : Yohann Burgan – Pascal Rullier
Animateur: Jérôme Bauzon

EGRA 2024

AGENDA

1. Définir la cybersécurité
2. Un enjeu de maîtrise des risques ?
3. Définir ce que vous souhaitez protéger
4. Comment améliorer la cybersécurité
5. Quels sont vos pratiques et outils ?
6. Et pour l'avenir

1.Définir la cybersécurité

Quelques définitions

- **Cybersécurité, n.f.**
  - État d'un système d'information qui résiste aux cyberattaques et aux pannes accidentelles survenant dans le cyberespace.
    La cybersécurité est assurée par la cyberprotection ainsi que, dans le cas d'un Etat, par la cyberdéfense.
- **Cyberattaque, n.f.**
  - Ensemble coordonné d’actions menées dans le cyberespace qui visent des informations ou les systèmes qui les traitent, en portant atteinte à leur disponibilité, à leur intégrité ou à leur confidentialité.
  - Une cyberattaque peut être ponctuelle ou s’inscrire dans la durée.

Quelques définitions

- **Cyberespace, n.m.**
  - Espace constitué par les infrastructures interconnectées relevant des technologies de l'information, notamment l'Internet.
- **Cyberprotection, n.f.**
  - Protection des ordinateurs, les serveurs, les appareils mobiles, les systèmes électroniques, les réseaux et les données contre les attaques malveillantes. On l’appelle également sécurité informatique ou sécurité des systèmes d'information

Quelques définitions

- **Cyberdéfense, n.f.**
  - Ensemble des moyens mis en place par un État pour défendre dans le cyberespace les systèmes d'information jugés d'importance vitale, qui contribuent à assurer la cybersécurité.
  - La cyberdéfense met notamment en œuvre la lutte informatique défensive et la lutte informatique offensive.

Quelques définitions

- **Cybermenace, n.f.**
  - Une cybermenace est un risque d’attaque de systèmes informatiques sur les infrastructures d'une compagnie, d'un État, d'une organisation privée ou publique, de son ou de ses systèmes d'information.

2.Un enjeu de maîtrise de risques

Analyse de risques

Choisir ce qu'on veut protéger et s'en donner les moyens

Objectifs :

- affirmer que tout système est faillible
- fixer les valeurs métiers essentielles
- connaître les menaces et adapter la stratégie
- définir la résilience des valeurs métiers face à des événements redoutés

Quelles sont les principales motivations des attaquants ?

- **L'appât du gain**
  - Les attaques à but lucratif visent à générer un gain financier de façon directe ou indirecte. Elles sont le plus souvent réalisées par des groupes de cybercriminels organisés.

Quelles sont les principales motivations des attaquants ?

- **Le pré-positionnement stratégique**
  - Après être parvenu à infiltrer un système d'information, l'attaquant peut décider de s'y installer. C'est ce que l'on appelle le pré-positionnement. Généralement, cela précède une attaque de longue durée dont la finalité n'est pas clairement établie. Ce pré-positionnement peut permettre à l'attaquant de conduire dans un second temps des actions de sabotage ou d'espionnage.

Quelles sont les principales motivations des attaquants ?

- **L'espionnage**
  - Les cyberattaques ayant une finalité de renseignement étatique ou économique sont le plus souvent réalisées en infiltrant les systèmes d’information d’une organisation ou d’un individu pour s’emparer des données qui y sont conservées et les exploiter.

Quelles sont les principales motivations des attaquants ?

- **La déstabilisation**
  - Les opérations de déstabilisation peuvent prendre plusieurs formes.
  - Certaines opérations d'influence reposent sur la compromission de contenus légitimes (boîtes mails, sites internet) afin de pouvoir les utiliser lors de campagne de diffusion de fausses informations. Ces contenus peuvent être altérés volontairement et diffusés publiquement.

La déstabilisation

- **Les attaques sur la chaine d'approvisionnement (supply chain attack)**
  - Ce type d'attaque consiste à compromettre un tiers, comme un fournisseur de services logiciels ou un prestataire, afin de cibler la victime finale. Cette technique est éprouvée et exploitée par plusieurs acteurs étatiques et cybercriminels depuis au moins 2016.

La déstabilisation

- **Attaque par rançongiciel**
  - Les attaques de type « rançongiciel » (ransomware) ciblent tous types d'organisations, y compris les acteurs publics et les services gouvernementaux. Très répandus, les rançongiciels sont des logiciels malveillants qui chiffrent l’ensemble des données, outils et applications de la victime (fichiers, messagerie, SAP, etc.). Pour les récupérer, cette dernière se voit demander le paiement d’une rançon en échange de la clé de déchiffrement. Les cybercriminels exfiltrent parfois les données internes de leur cible avant l’attaque, afin d’augmenter leur pression en menaçant de les publier.

La déstabilisation

- **Attaques par point d’eau**
  - L'attaque par point d'eau (watering hole) consiste à piéger un site internet légitime afin d’infecter les équipements informatiques des visiteurs. Elle peut aussi bien être employée contre des entreprises privées que des institutions travaillant sur des secteurs sensibles et qui disposent de systèmes informatiques hautement protégés et difficiles à attaquer.

La déstabilisation

- **Défiguration de sites internet**
  - Ce type d’attaque peut viser tout type d’organisation et exploite souvent des vulnérabilités connues mais non corrigées, pour ajouter ou modifier des informations dans une page web à des fins de revendications. Ces opérations sont généralement revendiquées par des hacktivistes pour motifs politiques ou idéologiques, ou à des fins de défi technique entre attaquants.

Quels sont les profils des attaquants ?

- **États et agences de renseignement**
  - Les États et agences de renseignements ont la capacité de réaliser une opération offensive de longue durée (ressources stables, procédures, etc.) et d'adapter leurs outils et méthodes à la typologie de la cible.

Quels sont les profils des attaquants ?

- **Organisations criminelles**
  - Du fait de la prolifération des kits d'attaques facilement accessibles en ligne et d'une spécialisation de l'offre technique sur le darknet, les organisations criminelles mènent des opérations de plus en plus sophistiquées et organisées, à des fins lucratives ou de fraude.

Quels sont les profils des attaquants ?

- **Hacktivistes**
  - Cette catégorie d'attaquant se distingue généralement par des attaques peu sophistiquées. L'objectif de ces individus est ainsi de véhiculer des messages et idéologies en ayant recours à différentes méthodes pour amplifier l'écho de leur action.

Quels sont les profils des attaquants ?

- **Entreprises spécialisées dans la vente de prestations et de services cyber-offensifs**
  - Ces officines sont généralement dotées de capacités informatiques élevées sur le plan technique et proposent de véritables services de piratage à leurs clients. Plusieurs offres de services sont possibles : des outils clé en main, de l'expertise humaine ou encore des capacités telles que des méthodes d'exploitation de vulnérabilités 0-Day. Si ces services sont généralement réservés à des clients étatiques dans le cadre de la lutte contre le terrorisme et la criminalité organisée, ils peuvent être détournés à des fins d'espionnage stratégique et politique à l'encontre d'autres cibles telles que des journalistes, des défenseurs des droits de l'Homme et de hauts responsables ainsi que d'entreprises détenant des données à caractère personnel ou stratégiques.

Quels sont les profils des attaquants ?

- **Amateurs**
  - Également appelés « script-kiddies », ces attaquants sont dotés de connaissances informatiques et motivés par une quête de reconnaissance sociale, d'amusement, de défi. Ils conduisent généralement des attaques basiques mais sont parfois à même d’utiliser les kits d’attaques proposés en ligne.

Quels sont les profils des attaquants ?

- **Menace interne**
  - Cette typologie d'attaquant peut être guidée par un esprit de vengeance aigu ou un sentiment d'injustice. Il peut par exemple s'agir d'un salarié licencié ou encore d'un prestataire mécontent suite au non renouvellement d'un marché.

3.Définir ce que vous souhaitez protéger

Atelier participatif

Quels sont les principaux actifs que vous souhaitez protéger, qu’est ce qui a le plus de valeur pour vous ?

Synthèse de l’atelier

- **Pourquoi la cybersécurité est-elle cruciale pour les radios associatives ?**
  - Protection des données sensibles
  - Prévention des interruptions de service
  - Maintien de la confiance des auditeurs et des partenaires

4.Comment améliorer la cybersécurité ?

Quelles sécurités à prendre ?

- **La sécurité réseaux**
  - Elle consiste à protéger le réseau informatique contre les intrus, qu'il s'agisse d'attaques ciblées ou de malwares opportunistes.
- **La sécurité des informations**
  - Elle veille à garantir l'intégrité et la confidentialité des données, qu'elles soient stockées ou en transit.

Quelles sécurités à prendre ?

- **La sécurité opérationnelle**
  - Elle comprend les processus et les décisions liés au traitement et à la protection des données. Les autorisations des utilisateurs pour l'accès au réseau et les procédures qui définissent le stockage et l'emplacement des données relèvent de ce type de sécurité.

Quelles sécurités à prendre ?

- **La reprise après sinistre et la continuité des opérations**
  - Elles spécifient la manière dont une entreprise répond à un incident de cybersécurité ou tout autre événement causant une perte des opérations ou de données. Les politiques de reprise après sinistre régissent la manière dont une entreprise recouvre ses opérations et ses informations pour retrouver la même capacité de fonctionnement qu'avant l'événement. La continuité des opérations se réfère au plan sur lequel s'appuie une entreprise tout en essayant de fonctionner sans certaines ressources.

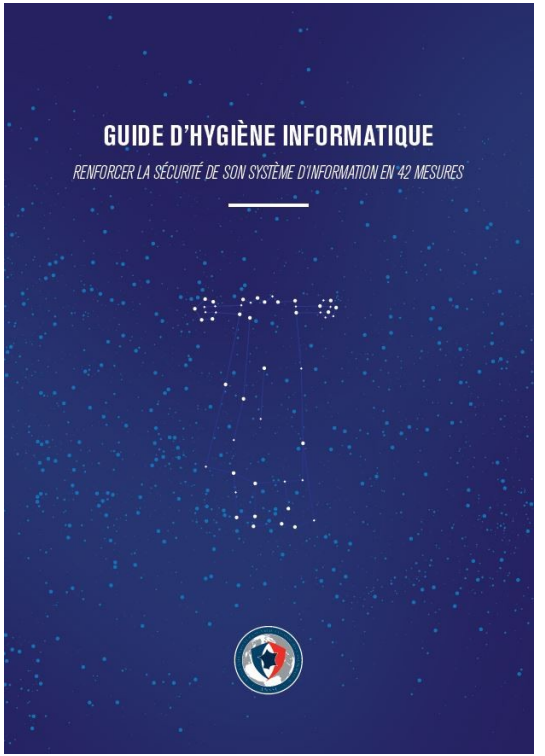
Quelles sécurités à prendre ?

- **La formation des utilisateurs finaux**
  - Elle porte sur le facteur le plus imprévisible : les personnes. Tout le monde peut accidentellement introduire un virus dans un système habituellement sécurisé en ne respectant pas les bonnes pratiques de sécurité. Apprendre aux utilisateurs à supprimer les pièces jointes suspectes et à ne pas brancher de clés USB non identifiées est essentiel pour la sécurité d'une entreprise.

Quelles sécurités à prendre?

- **Guide d’hygiène informatique de l’ANSSI**

https://cyber.gouv.fr/publications/guide-dhygiene-informatique



5.Quels sont vos pratiques et outils ?

Atelier participatif: Et dans vos radios ?

- **Comment mesurer le risque et prendre la décision du niveau de curseur pour investir dans des solutions de cybersécurité ?**
  - Définir les outils sensibles pour votre activité radio
  - Comment assurer votre activité radio en cas d'une cyberattaque ?

Et dans vos radios ?

- **Comment sensibiliser les équipes à ces enjeux ?**
  - Définir vos méthodes de travail
  - Formation des utilisateurs
  - Suivre le MOOC (Massive Open Online Courses)
    https://cyber.gouv.fr/le-mooc-secnumacademie

Et dans vos radios ?

- **Avoir de nouveaux réflexes ; mieux connaître les risques avec les outils que nous utilisons ?**
  - Lister tous les logiciels , systèmes d'exploitation, l'emplacement des données utilisés, l’accès à des services sur Internet

Et si cela vous arrive ?

- **Que faire en cas de cyberattaque ?**
  - Identification et isolation de la menace
  - Communication avec les parties prenantes
  - Restauration des services et des données

Cybersécurité

Questions / Réponses
Partage d’expériences
Tour de table

Pour aller plus loin

- https://cyber.gouv.fr/glossaire
- https://cyber.gouv.fr/tendances-les-cybermenaces
- https://cyber.gouv.fr/decouvrir-la-cybersecurite
- Panorama de la cybermenace 2023
  - https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-001.pdf

Cybersécurité

Merci de votre attention