CRESITT INDUSTRIE

Centre de Ressources
Technologiques en Électronique

Cybersécurité et Directive RED

EP/SR – 26/01/2023 – v1.0

Le CRT CRESITT est soutenu par :

L'action de diffusion technologique est cofinancée par l'Union européenne.
L'Europe s'engage en région Centre-Val de Loire avec le Fonds européen de développement régional.

Sécurisation

- Acte délégué pour renforcer la cybersécurité par rapport à la RED :

La Commission a publié le 29/10/2021 un acte délégué relatif à la directive RED, date de mise en vigueur : ***1er Aout 2024*** *:*

- *Garantir l'innocuité de tous les dispositifs sans fil par de nouvelles exigences, relatives aux garanties en matière de cybersécurité*
- *Objectifs : protéger la vie privée et les données à caractère personnel des citoyens, de prévenir des risques de fraude monétaire et de garantir une meilleure résilience des réseaux de communication.*

https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022R0030&from=FR

Sécurisation

Compléments de l' **Article 3 des« Exigences essentielles », point 3)** :

d) les équipements radioélectriques ne portent pas atteinte au réseau ou à son fonctionnement ni ne font une mauvaise utilisation des ressources du réseau, provoquant ainsi une détérioration inacceptable du service

→ Clarification : vrai pour tous les équipements connectés directement ou indirectement à internet

e) les équipements radioélectriques comportent des sauvegardes afin d'assurer la protection des données à caractère personnel et de la vie privée des utilisateurs et des abonnés

→ Clarification : vrai pour les équipements suivants si traitement de données à caractère personnel ou des données relatives au trafic et des données de localisation :

- Tous les équipements connectés directement ou indirectement à internet
- Tous les équipements destinés à la garde des enfants
- Tous les jouets
- Tous les « wearables »

Sécurisation

Compléments de l' **Article 3 des« Exigences essentielles », point 3)** (suite)

f) les équipements radioélectriques sont compatibles avec certaines caractéristiques assurant la protection contre la fraude;

→ Clarification : vrai pour tous les équipements connectés directement ou indirectement à internet qui permet au détenteur ou à l'utilisateur de transférer de l'argent, de la valeur monétaire ou une monnaie virtuelle

Évaluation de la conformité

Le règlement n'impose que des exigences essentielles (articles RED 3.3.d,e,f) qui sont formulées en termes généraux comme des objectifs à atteindre.

- Choix des solutions techniques spécifiques pour atteindre ces objectifs par les fabricants :
  - conforme aux normes harmonisées = auto-évaluation.
  - Si normes harmonisées non (entièrement) appliquées ou pas de normes harmonisées = évaluation par une tierce partie est obligatoire.
- La Commission européenne demandera une normalisation aux organisations européennes de normalisation… A suivre !

Exemple : transposition de la nouvelle directive Network and Information System Security (NIS 2) dans le droit français au deuxième semestre 2024

Sources :
https://www.agoria.be/fr/reglementation-finance/reglementation-technique/securite-et-compatibilite/cybersecurite-pour-les-equipements-radioelectriques-quelles-seront-les-obligations-legales

https://www.usine-digitale.fr/article/les-cyberattaques-visent-des-cibles-plus-faciles-comme-les-tpe-ou-les-sous-traitants-d-apres-l-anssi.N2092471

Exemples d'attaque sur objets connectés

- 2016 - Thermomètre connecté
  - accès réseau informatique
    - Liste clients

- 2017 - Caméras réseaux
  - zombie – attaque DDOS
    - Inaccessibilité DNS Dyn

- 2015-17 – Jouets connectés (poupée Cayla/barbie/teksta toucan)
  - Chercheurs – bluetooth sans password (cayla)
    - Accès micro – haut parleur

- 2015-16-18 – Voitures connectées (Jeep Cherokee,Tesla Model S-X)
  - Chercheurs – système info-divertissement (entertainment)
    - Accès auto-radio, lave-glace, air conditionné, commande moteur, autopilot

- 2019 – Trottinette (Xiaomi M365)
  - Faille de validation de l'authentification
    - Vérrouillage / déverrouillage à distance (100m)

- 2020 – machine à laver connectée Miele
  - Piratée → accès au système informatique d'un hôpital français → attaque de type rançongiciel bloquant tout l'établissement

- 2021/2022 : routeurs de marque Pakedge, Cyberoam, Cisco, MikroTik *(voir rapport ANSSI 2022)*

et aussi des lampes, aspirateurs, sonnettes sans fils, ….

Sécurisation

Norme EN 303 645 (pas harmonisée)

- Précise les bonnes pratiques en matière de sécurité des appareils IoT avec des exemples.
- Fournit un socle graduel de procédures de sécurité à mettre en œuvre vis à vis du niveau à obtenir
- Définit les mécanismes de base pour la protection contre les menaces de cybersécurité les plus courantes
- Dispositions (*provisions*) à essayer de respecter suivant les caractéristiques des objets (performances, composants matériels, autonomie…)
  - Dispositions axées sur les résultats
    - No Universal default password
    - Implement a mean to manage reports of vulnerability
    - Ensure software integrity
    - Keep software update
    - Securely store sensitive security parameters
    - Communicate securely
    - Minimize size of attack surfaces
    - Ensure that personal data is secure
    - Make system resilient to outages
    - Examine system telemetry data
    - Make it easy for user to delete user data
    - Make installation and maintenance device easy
    - Validate input data
    - Data protection provision for iot customer

processus de fabrication

produit

Solutions de sécurisation

Comment faire dans le produit ?

- Sécurisation du matériel
  - Fonctions intégrées
    - Secure element
    - Jtag sécurisé
    - Ressources de chiffrement
    - TrustZone

- Sécurisation logicielle
  - Bootloader sécurisé
  - Mémoires compartimentées
  - BlockChain
  - Trusted Execution Environment (TEE), MPU (Memoy Protection Unit), firewall, tamper detection,,,

Solutions de sécurisation

- Sécurisation du matériel
  - Microcontrolleur avec sécurisation
    - Exemples :
      - **ST Microelectronics** : **STM32L4x, STM32L5x** (PSA2), STM32U585 (PSA3 + SESIP3)
      - **NXP** : LPC55S69, LPC55S16 (PSA2)
      - **Renesas** : RA4M3, **RA6M4** (PSA2) , RA6M5, RX651
      - INFINEON (ex-Cypress) : PSoC 64 secure (PSA2)
      - Silicon labs : wireless gecko serie 2, EFR32MG21 (PSA3)
      - Infineon : Aptiga trust
      - Microchip : ATECC608A, SAM L11-KPH (PSA2)
      - Texas Instrument : Sitara AM43x
      - Nuvoto : NuMicro M2351

En gras : évalué par le CRESITT

Impacts de la sécurisation

- Impacts sur le produit
  - Consommation
    - Consommation supérieure avec SBSFU (Secure Boot Secure Firmware Update) et la trustzone et le chiffrement
  - Ressource mémoire
    - Besoin de plus de ressources mémoire (SBSFU)
  - Temps d'exécution
    - Temps de démarrage allongé par les vérifications du bootloader sécurisé
  - Prix
    - Plus cher qu'une solution sans sécurisation
    - Devrait certainement évoluer à la baisse à cause des régulations à venir et des normes existantes
      - NF EN IEC 62 443, NF EN IEC 61508, ETSI EN 303 645, ISO SAE 21434:2021…
  - **A mettre en perspective avec la responsabilité engagée du fabricant si une faille de sécurité est identifiée dans le produit** !

Projet régional

INSA CVL est lauréat du PIA4 « Campus des Métiers d'Avenir » avec le projet « CyberINSA », en partenariat avec le Campus des Métiers et des Qualifications ''Transformation Numérique'' et le CRESITT Industrie

Objectif : améliorer la compréhension des problématiques de cybersécurité au travers de différentes actions ciblant à chaque fois un public différent. Par exemple :

- Améliorer l'offre de formation et de sensibilisation dans la région
- Travailler l'attractivité des métiers de la cybersécurité
- Renforcer les transferts de la recherche pour favoriser l'expertise nationale dans le domaine de la cybersécurité et les transferts de technologies vers la formation et le monde professionnel.

Projet régional

Participation du CRESITT :

1. Fournir une plateforme de tests de résistance sur les objets connectés en radiofréquences

2. Participer à l'établissement des challenges sur des plateformes dédiées, puis les mettre en œuvre avec des industriels de tout domaine

3. Participer à la rédaction d'un guide d'évaluation de la sécurité des IoT

4. Réaliser des séminaires sur la sécurité des IoT

→ Lancement du programme courant février 2023 !

CONCLUSION

- **Formations CRESITT** :
  - Comprendre les contraintes et les enjeux d'intégration d'antennes 15/16 mars en présentiel et avec TP
  - CEM : comprendre les phénomènes : 20 juin en présentiel et avec démos
  - VHDL : 4 au 6 juillet en présentiel et avec TP

- Programme animation 2023 au CRESITT :
  - Séminaire «Capteurs et économies d'énergie »
  - Séminaire «IA et composants électroniques »
  - Atelier « Robots et drones »
  - Atelier « Interopérabilité » (aussi une des exigences de la Directive RED!)
  - Formations « design antenne RF, CEM, VHDL/traitement du signal, ...
  - Veille technologique sur les RISC-V et les composants pour IA

→ A suivre sur **www.cresitt.com**

CONCLUSION

- **Perform'Industrie** : accompagnements possibles en région Centre Val de Loire pour la cybersécurité (impacts fabrication) ou bien d'autres sujets…

  5 jours gratuits + 2*5 jours financés à 70 %, pour PME et ETI

  → Contactez-nous pour en savoir plus

- **QUESTIONNAIRES DE SATISFACTION**

  → à compléter en ligne , Merci !

- Vous souhaitez nous soutenir ? Adhérez au CRESITT 😉 !

  → www.cresitt.com/adherer

Contacts

Elisabeth PATOUILLARD / Christophe ALAYRAC

CRESITT Industrie, Lab'O, 1 avenue du Champ de Mars, CS 30019, 45074 Orléans Cedex 2

02 38 69 82 60 / 06 95 12 51 76 / 07 67 29 56 40

Elisabeth.patouillard@cresitt.com / Christophe.Alayrac@cresitt.com

Le CRT CRESITT est soutenu par :

Questions ?