Captronic Enova 15/03/2017

G-echo

Conseil, RH, Solutions, Diagnostics pour la cybersécurité.

Sécurité ...

Des failles ...

Attaque d'un device CAN par fuzzing

Failles

- Faille open SSL permet de déchiffrer le traffic https,
- Faille de la glibc ...
- Failles métier, par exemple contrôle de traffic aérien,

Exploits

- Hacking sans fil et (presque) sans les mains,
- Comment exploiter les failles des systèmes embarqués,
- Hack de caméra connectée,
- Kits d'exploitation des pirates.

Impacts

- JEEP et Mitsubishi dans l'(h)ac(k)tualité,
- Contrôle de véhicules par la liaison télématique,
- Infrastructures nucléaires vulnérables/rapport Suisse,
- Noyaux Linux avec backdoor.

mirai la carte

- 04/10/2016 code du botnet mirai (attaque IoT) libéré,
- **Explication sur no-limit secu !**,
- Une faille capable de bloquer Mirai ...

Solutions

Solutions systémiques

- Qu'est-ce que c'est la sécurité de l'information ?
- Six choses à faire en priorité,
- Documentation et livres blancs des autorités,
- Et bonnes pratiques.

Normes

- Famille ISO2700x : amélioration continue en SSI,
- Critères communs : niveau de sécurité d'un produit,
- CSPN : label français pour la sécurité des produits,
- ISA Secure : certification des systèmes industriels.

Test industriel en sécurité

- Test de sécurité en boîte noire,
- Démarche structurée et répétable,
- Rapports de conformité,
- Indépendant des technologies.

Test industriel de cybersécurité des systèmes

Nouveaux réseaux …

ANAJ SigFox VS Lora 09/03/2017

Conférences

La menace …

La menace

PaceMaker vulnérables/attaque boursière de StJude Medical.

Source ZdNet

Menace et opportunité

GDPR - règlementation européenne

- 72 heures pour déclarer un incident,
- 2 à 4% du CA mondial …

La menace ?

Class action, dommages et intérêts jusqu'à 3 M$, 10.000$ de dédommagements par client

Source Numerama

RETEX d'une PME

Une PME ...

- Entreprise < 3 ans,
- 3 ingénieurs sans connaissance de la cybersécurité,
- Développent leur électronique.

Stratégie

- Orientés grand public, ciblent les jeunes (<30 ans),
- Produit + services avec "gamification",
- Vision internationale.

Tactique

- Levée de fonds type crowdsourcing,
- Marché B2C évolue vers B2C rapidement ...

Et intéresse les assureurs (nature de l'activité de la société) ...

Opérationnel

- Partie physique du produit en vente et 80% conforme à audit de sécurité,
- Passés de quelques personnes à quelques dizaines de personnes.

Sécurité ?

- Protection des données personnelles mais également de l'usager,
- Vérification qu'une faille dans le système n'entraîne pas d'impact sur les systèmes autour (ne pas diminuer sécurité des systèmes hôté ou avec qui on communique),
- **GROS LEVIER EN B2B** ... non pardon ... **condition sine qua non ...**

Démarche ?

- Audit de gestion des risques pour TOUT le système

A ce moment là pas de spécialiste dans l'équipe … Audit réalisé par une société spécialisée.

Humilité

=> quels sont les points dans le système à améliorer ?

- Todo compliquée et longue.
- Besoin de design du sécurisé du système (fonctions techniques socle),
- Pas de miracle, répéter tous les jours (sensibilisation des équipes).

Humilité …

- Oui on va moins vite, mais nécessaire au fonctionnement de la boîte,
- Gens qualifiés, recrutement de gens qui savent ...

Aujourd'hui ?

- Ont maintenant mis en place les préconisation,
- Maturité => demandent à des gens externes de tester leur système,
- Réfléchissent à du bug bounty avec la difficulté qu'il y a un objet physique ?
- Banc de test HIL, physiquement localisé, mais pilotage à distance possible==> plateforme d'attaque.

Bilan

- Travail de terrain et de fourmi ...
- Il faut boucher partout, ne jamais s'arrêter de vérifier,
- Poser des barrières et vérifier tout le temps qu'elles n'ont pas été franchies...

Coût et justification ?

- Au moment de la levée et même encore maintenant,
- Investisseur dit : "les fonctionnalités utilisateur on peut en discuter (feature)".

Mais message sur socles techniques cyber-sécu = "Mettez l'argent qu'il faut pour que le système soit safe"

Numéro "0" de l'exigence.

Mais toujours très difficile de faire avaler la pilule du délai (très long à mettre en place, beaucoup d'efforts d'ingénierie).

- Pas une petite tâche.
- Par conception, impacte tout le système.
- Tout est plus long ...
- Les gens qui ne sont pas du métier ont du mal à le saisir ...

Bilan

Les investisseurs ont poussé pour être à la pointe sur le sujet et font des recommandations

Prônent la transparence totale (comment sont utilisées les données, comment elles circulent, acceptation, suppression, ...)

Et vous en cyber?

Auto-évaluation de votre niveau de sécurité.

Présentation des speakers

- 09h30-10h20 : Internet of Everything et sécurité ... par IRT-SystemX (Philippe WOLF),
- 10h20-11h10 : Internet des objets et sécurité: une mission impossible ? par DigitalSecurity (Damien CAUQUIL),
- 11h10-12h00 : Atteindre un bon niveau de sécurité avec Sigfox et LoRa par Sonia CORRARD (TSE et FAE Security chez SILICA)