IoT : Des lave-vaisselles sÃ©curisÃ©s ? BientÃ´t une nÃ©cessitÃ© ?
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 2/11/2017 14:30:00

Il y a quelques mois, une alerte de sÃ©curitÃ© a Ã©tÃ© Ã©mise concernant... un lave-vaisselle. Cet appareil commercial contenait en effet une vulnÃ©rabilitÃ© Directory Traversal critique qui aurait pu permettre aux pirates d'exploiter et d'accÃ©der Ã des informations sensibles.

Pire, aucun patch n'Ã©tait disponible pour cette faille, mettant ainsi en Ã©vidence un risque craint par de nombreux professionnels de la sÃ©curitÃ© : celui que des fabricants traditionnels cherchant Ã lancer leurs produits en premier ne soient pas en mesure de protÃ©ger ces appareils intelligents et connectÃ©s.

Â

Ã l'heure oÃ¹ la sÃ©curitÃ© passe encore souvent au second plan, les fabricants de produits grand public doivent aujourd'hui s'assurer d'avoir un plan de gestion des correctifs pour parer Ã l'Ã©ventualitÃ© d'une vulnÃ©rabilitÃ©.

Combler le fossÃ© avec les fabricants

Pour beaucoup, la dÃ©couverte d'une faille dans un lave-vaisselle est un exemple de plus d'un manquement au niveau de la sÃ©curitÃ© des consommateurs.

Pourtant, cela n'a rien d'une surprise... Les constructeurs du monde entier rivalisent afin d'intÃ©grer les toutes derniÃ¨res innovations Ã leurs produits, notamment pour en faire des appareils Â« intelligents Â».

L'essor de l'Internet des Objets (IdO) les pousse en dehors de leur zone de confort, en particulier pour ce qui est du dÃ©veloppement et de la sÃ©curitÃ© des logiciels.

Face Ã la prolifÃ©ration des produits connectÃ©s Ã Internet, les fabricants doivent dorÃ©navant mettre davantage l'accent sur la sÃ©curitÃ© lors de la phase de dÃ©veloppement.

Cela implique de tester minutieusement le code, d'assurer une maintenance en continu, de mapper soigneusement les logiciels intÃ©grÃ©s et de se tenir informÃ© de leurs potentielles vulnÃ©rabilitÃ©s. Il leur faut Ã©galement d'amples ressources pour rÃ©agir rapidement et efficacement le cas Ã©chÃ©ant.

Dans le cas de ce lave-vaisselle, il n'existait aucun patch connu. Ce genre de problÃ¨mes doit donc Ãªtre gÃ©rÃ© au cours de la phase de dÃ©veloppement.

Heureusement, de nouvelles technologies sont disponibles pour permettre aux constructeurs de dÃ©ployer des mises Ã jour forcÃ©es vers les clients (afin de rÃ©duire les vulnÃ©rabilitÃ©s et les risques potentiels).

Cependant, il leur faudra malgrÃ© tout mettre en place des stratÃ©gies de gestion des vulnÃ©rabilitÃ©s, c'est indispensable !

Beaucoup de fabricants n'ont tout simplement aucune idÃ©e des dÃ©fis concrets liÃ©s Ã l'IdO : aucun appareil connectÃ© Ã Internet n'est sÃ©curisÃ© Ã 100 %, et le risque de piratage ne peut jamais Ãªtre Ã©cartÃ©. Il est donc essentiel de mettre en place une stratÃ©gie de gestion des vulnÃ©rabilitÃ©s.

La sÃ©curitÃ© doit Ãªtre une prioritÃ© absolue

La sÃ©curitÃ© des applications doit Ãªtre la prioritÃ© des fabricants d'Ã©quipements : avec l'essor de l'IdO, les pirates lancent chaque jour des attaques plus sophistiquÃ©es.

Beaucoup de conseils ciblent les entreprises ou les consommateurs de dispositifs connectÃ©s. Cependant, si ces appareils ne sont pas sÃ©curisÃ©s, il n'y a pas grand-chose Ã faire.

La responsabilitÃ© est celle des fabricants, qui doivent fournir des applications sÃ©curisÃ©es ; faire en sorte qu'elles ne puissent pas Ãªtre piratÃ©es ; et Ãªtre en mesure de dÃ©ployer rapidement des mises Ã jour et des patches de leurs logiciels et firmwares.

La notion de sÃ©curitÃ© doit donc Ãªtre une considÃ©ration omniprÃ©sente. Il est important que ces processus soient stables, sÃ©curisÃ©s, et fonctionnent mÃªme au sein des Ã©cosystÃ¨mes IdO les plus Ã©tendus, lÃ oÃ¹ les logiciels font partie d'une chaÃ®ne d'approvisionnement plus vaste, ou dans les cas oÃ¹ ils seraient proposÃ©s aux cÃ´tÃ©s d'applications d'autres Ã©diteurs.

Les logiciels open source

Les logiciels open source sont frÃ©quemment utilisÃ©s par quasiment tous les dÃ©veloppeurs et dans pratiquement toutes les solutions IdO. MalgrÃ© leur omniprÃ©sence, ces composants ne font gÃ©nÃ©ralement l'objet d'aucune gestion, ce qui signifie que les dÃ©veloppeurs sont

incapables de suivre et de maÃ®triser les vulnÃ©rabilitÃ©s au niveau de leur code. L'analyse en

continu du code source leur permettra de conserver l'ensemble de ces composants tiers et open source Ã jour, et de rÃ©agir en cas de vulnÃ©rabilitÃ©.

Une fois ces logiciels dÃ©ployÃ©s, les applications devront Ãªtre rendues virtuellement inviolables afin qu'il soit extrÃªmement dur pour les pirates d'accÃ©der au code ou d'en faire quoi que ce soit. En outre, des technologies de sÃ©curisÃ©es et matures de gestion des licences devront Ãªtre appliquÃ©es afin que seuls les utilisateurs autorisÃ©s ne puissent y accÃ©der.

Enfin, des processus et technologies de mise Ã jour stables et Ã©volutifs devraient Ãªtre mis en place dÃ¨s le premier jour afin que les fabricants puissent mettre Ã jour les logiciels ou firmwares des appareils sur le terrain si un patch devenait nÃ©cessaire, ou en cas de piratage.

Trois conseils pour l'IdO (Internet des objets)

Les fabricants de dispositifs IdO devront suivre les trois conseils suivants pour assurer la sÃ©curitÃ© de leurs applications dans le monde de l'IdO :

1. Scanner le code base Ã la recherche d'OSS et de composants tiers potentiellement criblÃ©s de vulnÃ©rabilitÃ©s ;

2. ProtÃ©ger leurs applications du piratage Ã l'aide de systÃ¨mes de gestion des licences et des applications inviolables ;

3. Se tenir prÃªt Ã l'aide d'une solution de mise Ã jour automatisÃ©e et continue des logiciels et firmwares, et rÃ©agir rapidement lorsqu'une vulnÃ©rabilitÃ© nÃ©cessite d'Ãªtre corrigÃ©e ou en cas de piratage.

Pour conclure, Les dispositifs IdO sont de toute Ã©vidence de plus en plus intelligents. Mais comme souvent, l'innovation vient avec son lot de risques. Les fabricants et les organisations doivent donc continuer Ã se partager la tÃ¢che et prendre les prÃ©cautions nÃ©cessaires pour que leurs appareils ne deviennent pas une proie facile pour les criminels.

Houssem Ben Abderrahman - responsable Grands Comptes chez Flexera Software