Smart Things | Internet des objets

Cybersécurité: Défis pour la Suisse politique

Etat des lieux

L'internet des objets (IoT) peut être considéré comme une mise en réseau intelligente d'une infrastructure globale d'objets intelligents les plus variés dotés de fonctions les plus diverses (p. ex. capteurs de température, voitures, haut-parleurs, machines, etc.). La mise en réseau intelligente permet un nouveau lien entre ressources physiques et virtuelles avec possibilité d'interactions communes. Les possibilités qui en résultent permettent d'effectuer des actions automatisées, de collecter des informations et de les traiter ultérieurement.

Les termes Industrie 4.0 et OT (technologies opérationnelles) réunissent la quatrième révolution industrielle et l'utilisation de nouvelles technologies et possibilités techniques. Industrie 4.0[1] est considéré comme le terme générique du nouveau monde industriel, dans lequel les machines sont reliées les unes aux autres et interconnectées avec les technologies d'information et de communication les plus modernes. Grâce à la numérisation, les différents mondes et architectures des technologies de l'information (TI) et de l'OT traditionnelles sont de plus en plus interconnectés. Alors que l'informatique classique est utilisée pour le traitement de l'information, l'OT sert à contrôler les processus physiques dans la production industrielle et la logistique. Les systèmes d'OT hautement sensibles (p. ex. les centrales nucléaires), dont les systèmes informatiques sont exposés à l'internet, encourent ainsi de nouvelles nuisances potentielles et de nouveaux risques. Les maîtriser et y faire face représentent de grands défis et nécessitent également l'élaboration de nouveaux concepts. Les nouvelles technologies et la mise en réseau totale de l'OT et de l'IT entraînent des développements majeurs, de nouvelles possibilités d'application et des modèles économiques innovants dans les entreprises, l'administration et la société, pour autant que les risques associés soient gérés de manière appropriée et systématique.

Recommandations

1. Établir un aperçu de la situation actuelle et des développements futurs dans le secteur de l'IoT et faire connaître les bonnes pratiques existantes (le cas échéant, les normes et les structures).
2. Il convient de poursuivre une recherche approfondie sur la sécurité de l'IoT et de l'OT afin qu'elle puisse être garantie à l'avenir dans un environnement très hétérogène au moyen de nouveaux concepts et de nouvelles architectures.
3. La création et la normalisation de normes minimales dans les domaines de l'IoT et de l'OT à mettre en œuvre au moyen de réglementations appropriées. Une collaboration avec les organes compétents de l'UE aurait un impact bien plus fort.

[1] Le terme «Industrie 4.0» concerne bien plus la technologie IT/OT et se réfère principalement à de nouveaux concepts généraux tels que l'«usine intelligente» avec une mise en réseau complète des systèmes et des capteurs ainsi qu'une optimisation basée sur des données complètes ou la «maintenance prédictive» comme autre domaine.

Défis

Il est reconnu que l'utilisation de nouvelles technologies engendre des risques spécifiques. La mise en réseau à large échelle des objets intelligents physiques et virtuels augmente les risques sécuritaires et l'ampleur possible des dommages en raison de la zone d'attaque nettement plus étendue et de l'importance croissante de l'OT et de l'IT dans la création de valeur. Une attaque réussie sur un dispositif IoT peut impacter directement l'environnement réel/physique et, p. ex. entraîner une panne de courant, désactiver un stimulateur cardiaque ou endommager des installations industrielles. Face à cette évolution, les exigences en matière de sécurité deviennent plus élevées, p. ex. sous la forme d'une transmission et d'un stockage sécurisés des données. Aujourd'hui, les exigences accrues en matière de sécurité ne sont souvent pas reconnues ou délibérément ignorées (p. ex. dans le cas de l'IoT pour les applications privées) afin d'arriver sur le marché le plus rapidement possible avec un objet intelligent bon marché et pseudo-innovant. Cette situation signifie généralement que la sécurité des appareils et la vie privée des utilisateurs ne peuvent être suffisamment garanties. Dans le secteur du Consumer IoT (produits à usage privé), une défaillance du marché a été identifiée, les normes de sécurité étant insuffisantes.

Il convient également de noter que, dans l'environnement industriel en particulier, l'accent est clairement mis sur la sécurité (p. ex. la prévention des accidents) et non axée sur la sûreté (p. ex. les mesures de protection contre les attaques)[2]. En outre Et notamment dans le secteur de l'OT, la durée de vie des appareils utilisés est de plusieurs décennies, car ils sont souvent exposés à des charges physiques élevées dans des environnements difficiles. À titre de comparaison, d'autres objets intelligents sont parfois renouvelés après quelques mois (p. ex. les smart tags). Cette très grande palette d'exigences et de conditions-cadres doit être prise en compte afin de pouvoir développer et intégrer des systèmes globaux suffisamment sûrs.

La pratique actuelle montre que des concepts (p. ex. Security/Privacy by Design), des normes et des standards (p. ex. EN IEC 62443) communs et connus ne sont pas appliqués de manière cohérente ou n'existent même pas encore dans le domaine du développement de systèmes d'IoT et d'OT.

L'examen et la certification des composants et systèmes informatiques sont actuellement en cours de discussion en Suisse et au niveau de l'UE. Dans l'UE, une disposition légale en lien avec l'examen de la cybersécurité est actuellement débattue dans le cadre du Cybersecurity Act. En Suisse, les discussions tournent autour d'un concept de création d'un institut de contrôle en matière de cybersécurité pour les appareils interconnectés. Ces initiatives visent à obtenir une règlementation contraignante de la sécurité et de l'intégrité des produits numériques. Ces tests de qualité effectués par des organismes indépendants font depuis longtemps partie intégrante de l'autorisation des produits dans d'autres secteurs industriels sensibles tels que la technologie médicale.

Nécessité d'agir

Comme nous l'avons mentionné au début, le monde de l'IoT peut être divisé en deux grandes catégories:

– La mise en réseau de tous les objets intelligents possibles dotés de fonctions les plus variées
– Technologies opérationnelles (OT)/Industrie 4.0

Cette répartition en deux catégories requiert une manière d'agir propre à chacune.

En raison du manque de sensibilisation à la sécurité de certains fabricants d'objets intelligents ainsi que de la vision parfois angélique des

[2] Sécurité : être protégé contre les dangers non intentionnels, tels que les inondations ou les accidents. Sécurité : être protégé contre les actions malveillantes, telles que les menaces intentionnelles d'origine humaine, un vol ou une cyber-attaque.

utilisateurs, il est nécessaire d'aborder ces deux questions au moyen des champs d'action suivants:

Objets intelligents

– Appliquer la normalisation internationale et les certifications d'appareils correspondantes, notamment dans le domaine de la sécurité, afin d'augmenter la transparence (quel fabricant est certifié) et la sécurité (p. ex. Security/Privacy by Design). Sur cette base, prévoir une réglementation pour faire respecter un niveau de sécurité suffisant. Cette mesure doit être appliquée à large échelle dans la plus grande zone économique possible (p. ex. l'UE) afin d'influencer de manière efficace les grands fabricants.

– Soutenir le concept actuellement en discussion en Suisse pour la création d'un institut national de contrôle en matière de cybersécurité des appareils interconnectés et le promouvoir autant que possible.

– Poursuivre les initiatives de sensibilisation des utilisateurs afin d'accroître continuellement leur conscience des dangers liés à la sécurité.

– Recherche dans le domaine de la sécurité IoT/OT, notamment en ce qui concerne les concepts et les architectures permettant d'assurer la sécurité sur de très longues périodes d'utilisation (p. ex. une durée de vie de 30 ans).

OT/Industrie 4.0

— La mise en réseau croissante dans le domaine de l'OT pose un défi à chaque secteur économique, car il ne s'agit pas seulement d'intégrer de nouveaux systèmes, mais aussi d'interconnecter les (anciens) systèmes existants. En raison de la grande diversité des systèmes à interconnecter, qui ont également des exigences fondamentalement différentes en termes de sécurité, de disponibilité et de durée de vie, il est essentiel de disposer d'architectures de sécurité end-to-end adaptées et réalisables (p. ex. concept zéro confiance[3], microsegmentation). Afin d'empêcher la propagation éventuelle de la «shadow IT», les processus et interfaces informatiques existants doivent être adaptés en conséquence.

[3] Le concept de confiance zéro définit que toutes les connexions et tous les utilisateurs doivent être contrôlés à tout moment, qu'ils soient internes ou externes. La protection du seul périmètre du réseau n'est plus suffisante. "Ne faites confiance à personne, vérifiez tout". Voir aussi la rubrique inside-IT de Roger Halbheer (en allemand): https://www.inside-it.ch/de/post/satw-insights-zero-trust-sicherheit-in-zeiten-von-homeoffice-20200527

Références

- EN IEC 62443 - Réseaux industriels de communication – sécurité informatique des réseaux et des systèmes
- Ainsi que les normes ISA: https://www.isa.org/intech/201810standards/

Contact

Nicole Wettstein
Responsable du programme prioritaire Cybersécurité
+41 44 226 50 13

https://www.satw.ch/cybersecurity-defis

Impressum
Académie suisse des sciences techniques SATW
Contributions d'experts
Karl Aberer, EPFL | Umberto Annino, InfoGuard | Alain Beuchat, Banque Lombard Odier & Cie SA | Matthias Bossardt, KPMG | Adolf Doerig, Doerig & Partner | Stefan Frei, ETH Zürich | Roger Halbheer, Microsoft | Pascal Lamia, MELANI | Martin Leuthold, Switch | Hannes Lubich, Verwaltungsrat und Berater | Adrian Perrig, ETH Zürich | Raphael Reischuk, Zühlke Engineering AG | Riccardo Sibilia, VBS | Bernhard Tellenbach, ZHAW | Daniel Walther, Swatch Group Services | Andreas Wespi, IBM Research Lab
Rédaction et graphisme
Beatrice Huber; Claude Naville, Adrian Sulzer, Nicole Wettstein

www.satw.ch
Septembre 2020