GASTKOLUMNE

INTERNET DER DINGE EIN TEIL VON UNS

FRIDEL RICKENBACHER, MIT-GROUP
FRIDEL.RICKENBACHER@MIT-GROUP.CH

Einer der Mega-Trends «smart / connected homes» und letztlich das «Internet der Dinge» bieten zwar ein grosses Potenzial aber auch viele offenen Fragen.

Vor nicht allzu langer Zeit war das «unsichere» Internet auf Firmen- oder Heim-Computer begrenzt und isoliert. Mit der fortschreitenden Entwicklung von Internet- / Cloud-Lösungen und wachsender Mobilität mittels Smartphones, Notebooks und Homeoffice-Arbeit schwand die Grenze zwischen Privat und Business zunehmend.
Weitere Entwicklungen im Bereich der Heimvernetzung über Multimedia, Haushaltsgeräte, Haustechnik und letztlich «Internet der Dinge» werden dazu beitragen, dass wir nicht mehr nur ein Teil des Internets sind, sondern dass das Internet ein Teil von unserem privatesten Umfeld wird. Dass dann hierbei Unmengen von, hoffentlich erwünschten, Informationen im gesamten Haushalt, der Haustechnik, der Firmen- und Privat-EDV und speziell auch der Kinder-EDV fliessen werden, wird weitere Fragen und Herausforderungen der beherrschbaren Technologien und Sicherheit aufwerfen.

Immer wieder ist zu erfahren, dass bei den global führenden Lieferanten oder bei den Staaten hinterlegte Passepartout-Datenschlüssel vorhanden sind – ein beunruhigender Gedanke. Es muss aber auch beachtet werden, dass bei vielen Heimvernetzungssystemen oder teilweise auch bei Haustechnik-Steuerungsanlagen grundlegende Sicherheitsregeln wie z.B. Standard-Kennwort-Änderung, Deaktivierung von unnötigen Diensten etc. schon viel früher und trivialer zu mitverschuldeten Sicherheitslücken führen können. Auch werden viele neueste Innovationen und Technologien mitunter eher als tendenziell positiv und ohne Skepsis akzeptiert in der Annahme,

LA PAGE DE L'INVITÉ

L'INTERNET DES OBJETS UNE PARTIE D'ENTRE NOUS

FRIDEL RICKENBACHER, MIT-GROUP
FRIDEL.RICKENBACHER@MIT-GROUP.CH

L'une des méga-tendances «smart / connected homes» et au final «l'Internet des objets» offre un grand potentiel, mais laisse aussi de nombreuses questions ouvertes.

Il n'y a pas si longtemps encore, l'Internet «peu sûr» était limité aux ordinateurs de société ou de maison. Le développement progressif des solutions Internet et cloud ainsi que la mobilité croissante due aux smartphones, aux ordinateurs portables et au télétravail effacent de plus en plus les frontières entre le privé et le professionnel.
D'autres évolutions dans le domaine de la mise en réseau à domicile via multimédia, appareils électroménagers, techniques du bâtiment et au final «l'Internet des objets» feront en sorte que nous soyons plus seulement une partie d'Internet, mais qu'Internet devienne une partie de notre sphère la plus privée. Le flux d'énormes quantités d'informations – si possible – souhaitées dans l'ensemble du ménage, dans la technique du bâtiment, dans l'informatique d'entreprise et privée et notamment aussi dans l'informatique des enfants soulèvera d'autres questions et défis relatifs aux technologies contrôlables et à la sécurité.

On apprend sans cesse que les plus grands fournisseurs mondiaux ou les Etats disposent de clés de données passe-partout; cette idée est plutôt inquiétante. Cependant, il faut aussi tenir compte du fait que sur de nombreux systèmes de réseautage à domicile ou en partie aussi sur des commandes d'installations domotiques, des règles élémentaires de sécurité, par ex. le changement du mot de passe par défaut, la désactivation de services inutiles, etc., peuvent générer bien plus tôt des failles de sûreté imputables à une négligence. Aussi y a-t-il de nombreuses innovations et technologies dernier cri qui, d'une manière générale, sont acceptées immé-

dass es sich dabei ja um die neuesten und besten Errungenschaften handle. Aber auch hier muss mit der nötigen Sorgfalt geprüft werden ob, solche vernetzten Teilsysteme dann wirklich die erwünschten z.B. Stromverbrauchs-, Gebäudebewirtschaftungs- oder Gebäudenutzungsoptimierungen erzielen.
Was passiert, wenn solche «Smart-Devices» oder «Smart-Systems» durch Hersteller selber, unsauber programmierte Software-Versionen oder gar schadhaftem Code oder Hacker in die entgegengesetzte negative Richtung manipuliert werden? Hoffen wir einfach nur, dass künftig Hacker oder schadhafte Programm-Codes nicht «via Kühlschrank» zu uns kommen.

Ein weiteres ernsthaftes Grundproblem ist die anwachsende, beinahe gar blinde Systemgläubigkeit vieler Anwender. Diese kann dazu führen, dass man allen Anzeigen und Werten glaubt oder Folge leistet, ohne diese mit seinem gesunden Menschenverstand und natürlicher Skepsis zu hinterfragen. Auch darf man durchaus davon ausgehen, dass bei einem grösseren technischen Problem, einem Netzwerk- oder Internet-Problem, dann nur noch sehr wenig auf Anhieb funktioniert und das vermeintlich ausfallsichere, vollautomatisierte System sehr schnell zu einem eher halb-manuellen System mutiert. Hoffentlich wissen wir dann noch wie man von Hand die Fenster öffnet, falls das dann überhaupt noch geht.
Unsere «connected smart homes» mögen zwar irgendwann smart sein, ob sie aber aber auch wirklich - möglichst von Beginn an - genug sicher und beherrschbar sind, das sei dahingestellt. ■

http://fridelonroad.wordpress.com

diatement et sans la moindre réticence dans l'idée qu'il peut s'agir des dernières avancées techniques. Mais, là aussi, il faut vérifier avec toute la diligence requise que ces systèmes partiels interconnectés fournissent vraiment les optimisations souhaitées par ex. au niveau de la consommation d'énergie, de la gestion des bâtiments ou bien de l'utilisation des bâtiments.
Que se passe-t-il lorsque ces «smart devices» ou «smart systems» sont manipulés par les fabricants mêmes, par des versions de logiciel mal programmées, voire par un code défectueux ou un pirate, ce qui peut avoir l'effet négatif contraire? Espérons seulement qu'à l'avenir les pirates ou les codes de programme défectueux ne viendront pas chez nous «via le réfrigérateur».

Un autre problème fondamental sérieux réside dans la crédibilité technologique croissante, voire presque aveugle de nombreux utilisateurs. Il peut en résulter que l'on croit et se plie à toutes les informations et toutes les valeurs, sans même oser les remettre en question avec une dose de bon sens et de scepticisme naturels.
Aussi peut-on supposer qu'en cas de sérieux problème technique, de problème de réseau ou Internet, peu de choses ne fonctionneront d'emblée et que le système entièrement automatique et supposé protégé contre les défaillances se transformera très rapidement en système plutôt semi-manuel.
Espérons que nous saurons alors encore comment ouvrir une fenêtre à la main si cela est encore possible.
Avant même de se poser la question de savoir si nos maisons intelligentes connectées seront un jour vraiment intelligentes, il faut qu'elles deviennent suffisamment sûres et contrôlables. ■

http://fridelonroad.wordpress.com

Fridel Rickenbacher ist Mitbegründer, Partner und Verwaltungsrat der *MIT-Group,* einem Totalunternehmen für Informations- und Kommunikationsmanagement. Er absolvierte seine Ausbildung in den Bereichen Bauleiter/Projektleiter/Immobilienverwaltung (*FH Horw*) und Wirtschaftsinformatik/Engineering (*HSLU*) und ist seit über 13 Jahren Mitglied in der Informatikkommission des SIA.

Fridel Rickenbacher est cofondateur, associé et membre du conseil d'administration de *MIT-Group*, une entreprise totale de gestion de l'information et de la communication. Il a une formation de chef de chantier, chef de projet, administrateur immobilier (*FH Horw*) et en informatique économique, ingénierie (*HSLU*) et il est depuis plus de 13 ans membre de la commission informatique de la SIA.

In den Gastkolumnen publizieren wir jeweils die Meinung wechselnder Autoren zu aktuellen Themen. Es handelt sich dabei weder um die Meinung der Redaktion, noch um die Haltung des SIA.

Dans les colonnes de l'invité, divers auteurs s'expriment sur des thèmes actuels. Leurs réflexions n'engagent pas la Rédaction et ne reflètent pas les positions de la SIA en la matière.