Zeitschrift: Bulletin Electrosuisse
Herausgeber: Electrosuisse, Verband für Elektro-, Energie- und Informationstechnik
Band: 105 (2014)
Heft: 4

Artikel: Solide Basis für sichere Computer = Une base solide pour des ordinateurs sûrs
Autor: Weber, Arnd
DOI: https://doi.org/10.5169/seals-856219

FORUM

Solide Basis für sichere Computer

Arnd Weber
ist Senior Scientist am Karlsruher Institut für Technologie (ITAS)

Die Computersicherheit ist ein Domäne, bei der man permanent nachbessert. Es ist weder klar, was in den Maschinen ist, noch ob Geschäftsgeheimnisse und Infrastrukturen gegen Angriffe geschützt sind. Mit professioneller Hilfe kann ein meist ausreichend sicherer Zustand erreicht werden. Die Zukunft wird noch unsicherer: Organisationen wie Geheimdienste bauen sicherheitsrelevante Schwächen ein, und mit Trojanern in der Hardware muss gerechnet werden. Für eine sichere Computer-Nutzung müssen folgende Fragen behandelt werden:

Erstens möchte man vorhandene Anwendungen weiternutzen. Offene Systeme sind erwünscht, damit neue Anwendungen möglich sind. Wenn aber jedermann Programme entwickeln kann, sind Fehler und Angriffe möglich. Der Ausweg: Anwendungen zu isolieren, damit Schadprogramme weder heraus- noch hineinkönnen. Die Anwendung solcher Container bedeutet aber Umlernen, denn Clipboards funktionieren nicht oder kommen unter die Kontrolle der zentralen Administratoren.

Zweitens ist das Ziel schwer erreichbar. Alle Systeme müssen gründlich evaluiert werden. Laufend kommen neue Anwendungen und Peripheriegeräte hinzu. Stets muss man mit neuen Angriffen rechnen, z.B. mit der Nutzung von «Seitenkanälen» zum Abhören. Trotzdem ist es sinnvoll, das Ziel anzustreben, um Angriffe auf Infrastrukturen, Geschäftsgeheimnisse oder Bankkonten abzuwehren.

Drittens ist es teuer, das Ziel zu erreichen. Verbessert ein Anbieter eine Komponente, einen Chip oder einen Teil eines Betriebssystems erheblich, ist er dem Risiko ausgesetzt, dass seine Kunden hierfür nicht viel zahlen, zumal er die Sicherheit des Gesamtsystems nicht garantieren kann. Wie soll so ein sicheres Gesamtsystem entstehen?

Am Karlsruher Institut für Technologie wird deshalb diskutiert, ob der Staat Vorschriften machen sollte, damit die gesamte Branche Anreize erhält, immer bessere Komponenten und Systeme zu bauen. Unser Institut hat beispielsweise eine Konferenz beim Europaparlament organisiert, an der technische Experten solche regulatorischen Massnahmen diskutierten. Weitere Schritte müssen natürlich folgen, um dem Ziel näher zu kommen.

Une base solide pour des ordinateurs sûrs

Arnd Weber
Senior Scientist à l'Institut de technologie de Karlsruhe (ITAS)

La sécurité informatique constitue un domaine continuellement en cours d'amélioration. Il est en effet difficile non seulement de savoir ce qu'il y a dans les machines, mais aussi d'être certain que les secrets commerciaux et les infrastructures sont bien protégés contre les attaques. Une assistance professionnelle permet toutefois d'obtenir une sécurité suffisante la plupart du temps. L'avenir deviendra cependant encore moins sûr. Des organisations telles que les services secrets introduisent des faiblesses en matière de sécurité et il faudra compter sur la présence de chevaux de Troie dans le hardware. Pour une utilisation sûre des ordinateurs, il sera nécessaire de traiter les questions suivantes.

Premièrement, nous aimerions continuer à utiliser les applications existantes, ainsi que des systèmes ouverts afin de permettre le développement de nouvelles applications. Si tout un chacun est cependant en mesure de concevoir des programmes, les erreurs et les attaques restent possibles. La solution : isoler les applications afin d'empêcher les logiciels malveillants d'y entrer ou d'en sortir. L'application de tels conteneurs nécessite néanmoins un changement de comportement car les presse-papiers ne fonctionnent alors plus ou sont contrôlés par les administrateurs centraux.

Deuxièmement, un tel objectif est difficilement réalisable. Tous les systèmes doivent faire l'objet d'une évaluation approfondie. De nouvelles applications et de nouveaux périphériques ne cessent de venir s'ajouter à ceux déjà existants. Il faut compter en permanence sur de nouvelles attaques, par exemple des attaques par canal auxiliaire (side channel attacks) à des fins d'écoute. Il est néanmoins judicieux de poursuivre l'objectif consistant à repousser celles visant les infrastructures, les secrets commerciaux ou les comptes bancaires.

Troisièmement, la réalisation d'un tel objectif a un prix. Si un fournisseur améliore considérablement un composant, une puce ou une partie d'un système d'exploitation, il s'expose au risque suivant : ses clients ne paieront qu'une faible somme en contrepartie de cet effort, d'autant plus que le fournisseur ne sera pas en mesure de garantir la sécurité du système dans sa globalité. Comment mettre ainsi sur pied un système global sécurisé ?

Des discussions sont menées à l'Institut de technologie de Karlsruhe afin de savoir si l'État devrait établir des prescriptions visant à inciter la branche à construire de toujours meilleurs composants et systèmes. À titre d'exemple, notre institut a organisé une conférence au Parlement européen au cours de laquelle des experts techniques ont discuté de telles mesures réglementaires. Plusieurs étapes supplémentaires devront suivre, bien entendu, afin de se rapprocher de l'objectif fixé.