Philippe Vuilleumier
Chief Security Officer, Swisscom

Hacker im Haus

Die digitale Vernetzung von Systemen und Services bildet die Basis für clevere Gebäudeleitsysteme. Über sie erfolgt die Steuerung von Heizungs-, Lüftungs- und Lichtsystemen, aber auch Notstromanlagen und Computernetzwerke werden darüber verbunden. Sie ermöglichen nicht nur ein modernes Gebäudemanagement, sondern helfen auch, Energie und Kosten zu sparen.

Mit zunehmender Vernetzung steigt allerdings auch das Risiko einer gewollten oder ungewollten Fehlmanipulation. Es gibt unzählige Praxisbeispiele, die zeigen, wie Cyberkriminelle physische Objekte, die mit dem Internet verbunden sind, sogenannte IoT-Devices, gezielt missbrauchen.

So sorgte im Oktober 2016 die Schadsoftware Mirai (japanisch: Zukunft) für einen Riesenwirbel, denn mit ihr liessen sich Botnetze aufbauen. Dazu scannte Mirai das Internet nach Sicherheitslücken auf IoT-Geräten (Babyphones, WLAN-Kameras, TVs etc.) ab und versuchte, Schadcode auf sie aufzuspielen. Die Hacker nutzten die Devices, um gezielte Attacken durch absichtliche Überlastungen von Netzen – sogenannte DDoS-Attacken – zu provozieren. Dabei waren sie sehr erfolgreich. Es gelang ihnen, den Dyn-Dienst im Internet durch mehrere Millionen gleichzeitiger Anfragen zu überlasten. Zu den bekannten Webseiten, die während des Angriffs offline gingen, zählten CNN, Netflix und die BBC.

Hat sich die Situation in den letzten fünf Jahren verbessert? Leider nein! Suchmaschinen wie Shodan lassen erahnen, wie viele Geräte immer noch ungeschützt über das Internet erreichbar sind. Die in Shodan verzeichneten Devices reichen von Haushaltsgeräten bis zu Industrieanlagen. Um diese sehr unterschiedlichen Systeme sicherer zu machen, bedarf es noch grosser Anstrengungen. Wahrscheinlich werden auch neue, weltweit gültige Vorgaben nötig sein, um diese Bedrohung langfristig zu beseitigen.

Während das Cyberrisiko bei Neubauprojekten von Anfang an mitberücksichtigt werden kann, gilt es, dieses auch bei Renovationen miteinzuplanen. Zum Glück gibt es dafür bereits ein gutes Angebot an Lösungen und entsprechende Anbieter.

Des hackers à la maison

La mise en réseau numérique des systèmes et des services constitue la base des systèmes intelligents de gestion des bâtiments. Ces derniers sont utilisés pour contrôler les systèmes de chauffage, de ventilation et d'éclairage, mais aussi pour connecter les systèmes d'alimentation de secours et les réseaux informatiques. Ils permettent non seulement une gestion moderne des bâtiments, mais aident également à économiser de l'énergie et de l'argent.

Cependant, plus la mise en réseau s'étend, plus le risque d'une mauvaise manipulation augmente, que celle-ci soit intentionnelle ou non. Il existe d'innombrables exemples de cas qui montrent comment les cybercriminels utilisent de manière ciblée des dispositifs IoT, c'est-à-dire des objets physiques connectés à Internet.

En octobre 2016, par exemple, le logiciel malveillant Mirai (« futur » en japonais) a fait grand bruit, car il a pu être utilisé pour mettre en place des botnets. Mirai scannait l'Internet à la recherche de failles de sécurité sur les appareils IoT (moniteurs pour bébés, caméras Wi-Fi, téléviseurs, etc.) et tentait d'y installer du code malveillant. Les hackers ont utilisé ces dispositifs pour provoquer des attaques ciblées en surchargeant délibérément les réseaux, ce que l'on appelle des attaques DDoS, et ce, avec grand succès. Ils ont réussi à surcharger le service Dyn sur Internet en faisant plusieurs millions de demandes simultanées. Parmi les sites Web connus qui ont été mis hors ligne lors de l'attaque figurent CNN, Netflix et la BBC.

La situation s'est-elle améliorée au cours des cinq dernières années ? Malheureusement pas ! Des moteurs de recherche comme Shodan donnent une idée du nombre d'appareils encore accessibles sans protection sur Internet. Les dispositifs répertoriés dans Shodan vont des appareils ménagers aux installations industrielles. De gros efforts sont encore nécessaires pour augmenter la sécurité de ces systèmes si différents. De nouvelles directives applicables au niveau mondial seront probablement aussi nécessaires pour éliminer cette menace à long terme.

Si dans les nouveaux projets de construction, les cyberrisques peuvent être pris en considération dès le début, ils doivent également être pris en compte dans les rénovations. Heureusement, pour ce faire, il existe déjà un bon éventail de solutions et des fournisseurs en conséquence.