Breitband/IT

Auf dem Weg zum sicheren Smart Home.

Immer mehr Funktionen in Häusern lassen sich über das Internet steuern. Das »Smart Home« verspricht effizientes Gebäudemanagement. Doch die Systeme sind in vielen Fällen nicht sicher und lassen sich nur mit großem Aufwand erneuern. Forscher arbeiten an einer Software, die Hackerangriffe abwehrt, bevor sie die Gebäude erreichen.

Auf dem Weg zum sicheren Smart Home; Foto Fraunhofer

Botnets

Botnet. Ein Begriff aus der Computerwelt schleicht sich langsam in die Welt der Gebäudeautomation. Mit diesem Angriffsszenario ist laut Dr. Steffen Wendzel von der Bonner Abteilung »Cyber Defense« des Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergonomie FKIE in Wachtberg zu rechnen. Der Forscher aus der ist Experte für die Hackermethode und hat sie zusammen mit Viviane Zwanger und Prof. Dr. Michael Meier unter die Lupe genommen. Angreifer infiltrieren dabei mehrere Rechner – Bots (von engl. robots) – ohne die Kenntnis ihrer Eigentümer, schließen sie zu Netzen (engl. nets) zusammen und missbrauchen sie für Computerattacken. Die Forscher untersuchten, was es aktuell noch gar nicht gibt: Angriffe durch Botnets auf »Smart Homes«, mit dem Internet vernetzte Gebäude bzw. Gebäudefunktionen. Das Ergebnis: Die Bedrohung ist real, über das Internet gesteuerte Rollläden, Heizungen oder Schließsysteme können für derartige Attacken genutzt werden. »Unsere Experimente im Labor zeigten, dass Gebäude-IT nicht ausreichend gegenüber Angriffen aus dem Internet geschützt ist. Ihre Netzwerkkomponenten können als Botnet missbraucht werden«, so Wendzel. Der Hacker hat es dabei nicht wie bisher auf PCs abgesehen, sondern auf diejenigen Komponenten der Gebäudeautomation, die Häuser mit dem Internet verbinden. Das sind im Gebäude verbaute, kleine Kästchen, die ähnlich wie Router für den Heimcomputer aussehen und funktionieren. »Sie sind jedoch sehr einfach aufgebaut, können nur schwer aktualisiert werden und weisen Sicherheitslücken auf. Die Kommunikationsprotokolle, die sie nutzen, sind veraltet«, so Wendzel.

Schutzsoftware schaltet sich zwischen Internet und Gebäude-IT.

Datenverkehr

Damit die Heizung, die Beleuchtung oder die Lüftung von Gebäuden über das Internet gesteuert werden können, ist es notwendig, spezielle Technik zu installieren: Es handelt sich dabei um kleine Minicomputer, die Temperaturen, Licht oder Luftfeuchtigkeit messen und in Netzwerken zusammengeschlossen sind. »Sie sicherheitstechnisch auf dem neuesten Standard zu halten, ist teuer«, sagt Wendzel. Am FKIE entwickelte das Team eine Schutzsoftware, die sich einfach zwischen Internet und Gebäude-IT schalten lässt. Die Technologie filtert potentielle Angriffe aus den Kommunikationsprotokollen heraus, noch bevor sie die eigenen vier Wände oder das Bürohaus erreichen. Ganz egal, welche Technik innerhalb der Gebäude verwendet wird: Sie muss bei dieser Herangehensweise nicht ausgetauscht werden.

Die Forscher nahmen dazu den gängigen Kommunikationsstandard der Gebäudeautomation unter die Lupe und entwickelten darauf aufbauend Regeln für den Datenverkehr. Halten eintreffende Daten diese nicht ein, wird der Kommunikationsfluss angepasst. »Die Software funktioniert wie eine Firewall mit Normalisierungskomponente«, sagt Wendzel. Ein »Analyzer« prüft sämtliche Ereignisse auf Plausibilität, die auf den Weg zu den Systemen geschickt werden. Schlägt er Alarm, geht der Vorfall unmittelbar an den »Normalizer«. Dieser blockiert das Ereignis entweder ganz oder wandelt es passend um. »Die Grundlagenforschung ist erfolgreich abgeschlossen. Im nächsten Schritt wollen wir die Technologie zusammen mit einem Industrieunternehmen zur Produktreife bringen. In spätestens zwei Jahren sollte ein Produkt auf dem Markt sein«, sagt Wendzel.

Bei ihrer Analyse der Botnet-Angriffe skizzierten die Forscher konkrete Bedrohungsszenarien für Smart Homes. »Aus meiner Sicht ist das Thema ›Überwachung‹ das drängendste«, sagt der Cyber Defense-Forscher. Indem der Angreifer sich in die IT von Gebäudefunktionen hackt, erfährt er im schlimmsten Fall, wo die Insassen sind und was sie machen. Das reicht dann bis zum Gang auf die Toilette. Einbrecher, zum Beispiel, könnten die Daten nutzen, um ihre Raubzüge vorzubereiten. Hier agiert der Hacker passiv, zapft Informationen an. Er wäre aber genauso gut in der Lage, aktiv in die Systeme einzugreifen. Zum Beispiel für einen Auftraggeber aus der Energiebranche. Der könnte von mehr verkauftem Öl oder Gas profitieren, wenn der Verbrauch mehrerer Heizungen künstlich erhöht wird. Wie real dieses Szenario ist, zeigt ein aktuelles Beispiel: Im vergangenen Jahr gab es eine Lücke im Sicherheitssystem einer an das Internet angeschlossenen Heizung. Angreifer hatten die Möglichkeit, die Heizkörper auszustellen oder zu beschädigen. Momentan rät Sicherheitsexperte Wendzel deshalb davon ab, Gebäudefunktionen in Eigenheimen allzu sorglos mit dem Internet zu verbinden.

Fraunhofer