


Perícia Digital e a Domótica: Casa inteligente, riscos e crimes digitais

A Domótica é uma nova tecnologia que permite a gestão de todos os recursos habitacionais, simplificando a vida das pessoas. O termo “Domótica” resulta da junção da palavra latina “Domus” (casa) com “Robótica” (controle automatizado de um ambiente).

Embora tenha nascido em um contexto militar, hoje vivenciamos o crescimento das tecnologias nos ambientes domésticos. A máxima aqui é o controle de iluminação, climatização, e principalmente, segurança, de forma interligada. Outros elementos e dispositivos eletrônicos também podem ser interligados. Um dos principais controles utilizados no mundo é o Z-Wave (<http://www.z-wave.com/modules/AboutZ-Wave/>), onde os especialistas são cada vez mais requisitados no mercado brasileiro. 

O que antes era privilégio de milionários, hoje pode integrar casas e ambientes corporativos por menos de dois mil reais (sistemas básicos), sendo que segundo o jornal Folha de São Paulo, os kits já estão cerca de 60% mais baratos que há três anos

(<http://www1.folha.uol.com.br/mercado/888088-casa-inteligente-chega-a-classe-media.shtml>)

A automatização das tarefas de uma casa ou ambiente corporativo, pressupõe a existência de uma central de controle, esta que pode ser conectada a um pc ou mesmo se comunicar por meio de Internet. Fala-se hoje em “domótica inteligente” onde os sensores de um ambiente residencial ou corporativo poderiam conhecer o comportamento daqueles que lá

habitam ou trabalham, no conceito chamado “ABC”, automação com base no comportamento.



Esquema de recursos passíveis de controle pela Domótica

A característica da domótica é a integração de dispositivos em um único controlador. Tal ponto, se por um lado organiza a gestão das “casas virtuais”, por outro permite que todo um sistema seja perturbado em uma única investida, que pode, assim como na alteração de um firewall, alterar ou criar regras no sistema inteligente, prejudicando os que dele se valem.

Logicamente que ataques a estes sistemas residenciais poderão ser feitos por pessoas que conhecem as intimidades do projeto eletrônico, por outro lado, deve-se pontuar que ter uma casa automatizada na Internet será um risco que precisará levar em consideração critérios no escopo de minimizá-lo.

Que a domótica vem tornar a vida mais fácil não há dúvida. O mesmo não se pode dizer quanto à segurança. Os sistemas passam a reagir por uma ordem dada por um interruptor ou por um comando, que pode ser remoto, até mesmo via celular.

Neste cenário, novas ameaças surgem na sociedade da informação. Um criminoso digital pode, por exemplo, cancelar ou paralisar sistemas de irrigação automática, prejudicando hortas e plantas, superaquecer a água para o banho, desligar a aspiração central ou purificador de ar, bem como iluminação, preparando o ambiente para um ataque ou assalto físico, o que pode ser fatal aos habitantes e pessoas que ali trabalham.

Igualmente, um agressor pode desligar os níveis de segurança, tornando indisponíveis sensores de gás, inundações, incêndios, bem como o sistema de comunicação com autoridades e com os

proprietários. Sistemas de monitoramento, controle de acesso por impressão digital e padrão retinal ou de voz também podem ser prejudicados. Em síntese, se antes o criminoso usava uma chave ou alicate para cortar as correntes, cercas elétricas e cadeados de uma casa, em breve, bastará conhecimentos de tecnologia e alguns comandos, executados remotamente.

Deve-se mencionar também, que a domótica pressupõe central de conectividade (Internet), integrando dados com comutação de tomadas e energia. Se alteradas por um criminoso, poderia expor dados de seus moradores ou mesmo servir de ponte para a prática de outros crimes digitais.

Como se verifica, a domótica ao colocar a casa ou ambiente corporativo na Internet, traz consigo diversas ameaças. Empresas que façam automação deverão pensar em segurança, envolvendo atualização constante do *middleware* dos equipamentos e riscos de invasões, alterações indevidas e outras possibilidades. A questão da responsabilização civil dos fornecedores também deverá vir à tona, onde os titulares de residências inteligentes poderão ser valer de perícia especializada para apurar o responsável por vulnerabilidade no sistema que tenha permitido a atuação de um criminoso ou a consumação de um incidente.

A segurança eletrônica será em breve parcialmente absorvida pela segurança da informação, o que demandará atualização dos profissionais pois até mesmo uma residência deverá ter um firewall lógico configurado e atualizado, ou será presa fácil do crime da era da sociedade da informação.

José Antonio Milagre é Advogado e Perito especializado em Segurança da Informação. E-mail: jose.milagre@legaltech.com.br
– Twitter: <http://www.twitter.com/periciadigital>