Smart meters e sicurezza informatica, case a rischio cyber attacchi secondo l'intelligence britannica

Un piano da 11 miliardi di sterline per installare contatori intelligenti (***smart meters***) nelle case dei cittadini britannici. Il Governo del Regno Unito, come molti altri Paesi europei, punta così ad una trasformazione digitale sul territorio che faccia leva anche sull'**efficienza energetica**.

Gli *smart meters* consentono agli utenti di tenere sotto controllo i consumi e quindi ridurli. L'**inquinamento atmosferico** che sta soffocando le città e rendendo sempre più caldo il pianeta deriva in gran parte proprio da sistemi di riscaldamento scarsamente efficienti per sprechi, perdite e comportamenti poco virtuosi dei cittadini stessi.



Secondo quanto annunciato dal Governo di Londra a gennaio di quest'anno, i lavori per l'installazione di questi contatori di nuova generazione saranno terminati nel 2020. Al momento, ha riportato il quotidiano *The Telegraph*, le abitazioni con *smart meter* attivo sono 8 milioni di unità su 27 milioni totali.

Fin qui tutto bene, ma la *Government communications headquarters* (**Gchq)**, l'agenzia governativa che si occupa della sicurezza, nonché dello spionaggio e controspionaggio, nell'ambito delle comunicazioni del Regno Unito, ha lanciato un nuovo allarme nei giorni scorsi, relativo alla **cyber sicurezza** di queste apparecchiature. Essendo questi *smart meters* sempre connessi in rete, anche per l'invio di dati sui consumi ai fornitori di energia, il loro livello di sicurezza informatica è costantemente messo alla prova dai cyber criminali.

Proprio a causa dell'alto rischio di attacchi informatici è stato rimandato il lancio dei nuovi contatori digitali **Smets 2**.

L'Agenzia ha indirettamente puntato il dito anche sull'***internet of things*** e la sicurezza domestica: sfruttando le vulnerabilità dei contatori l'attacco informatico potrebbe rapidamente estendersi al resto della casa e dei device interconnessi tra loro.

I cyber criminali sono così messi in condizione di danneggiare i fornitori di luce elettrica e gas e i consumatori stessi, a cui peraltro potrebbero esser sottratti soldi sui conti correnti e qualsiasi tipo di informazione sensibile.

Come ha spiegato a *The Mail* l'esperto informatico di WiFore, **Nick Hunn**: "*Il problema è che il piano di attivazione degli smart meter è portato avanti da funzionari in carriera che poco sanno di cyber sicurezza e poco si curano delle possibili conseguenze in termini di danni economici e materiali che potrebbero subire aziende e cittadini*".

Completamente diversa è l'opinione dell'agenzia governativa **Smart Energy GB**, preposta alla realizzazione del piano *smart meter* per la Gran Bretagna: "*I contatori intelligenti sono assolutamente sicuri ed affidabili, solo i dati energetici sono registrati dal dispositivo, e comunque sono*

crittografati. Il resto delle informazioni personali, dall'indirizzo al conto bancario, non sono accessibili tramite contatore".

La Gchq, dal canto suo, ha precisato: "*Sicuramente lo Smart metering system troverà presto il giusto equilibrio tra sicurezza informatica e business, nel rispetto dei più ampi obiettivi di politica e sicurezza nazionale*".

> *Smart meters e sicurezza informatica, case a rischio cyber attacchi secondo l'intelligence britannica*