I giocattoli smart sono pericolosi?

Ricevuto uno splendido smart toy per Natale? Occhio: la privacy è a rischio

di **Riccardo Meggiato**
(http://www.wired.it/author/rmeggiato)
27 DIC, 2016

Per il 2020 si stima che il 90% delle auto prodotte sarà collegato a Internet. Per allora, del resto, a sancire il successo all'Internet of Things (IoT), ci saranno oltre 50 miliardi di dispositivi connessi. **E tra questi, pure un sacco di smart toy.** Parliamo di giocattoli che sfruttano la Rete per offrire funzioni avanzate, come per esempio il riconoscimento della voce. Bambole che dialogano in modo realistico col bambino, auto radiocomandate che eseguono percorsi programmati via web, robot dotati di videocamera che permette ai genitori di controllare i figli a distanza.

Tutto molto bello e moderno, ma visto che parliamo proprio di dispositivi IoT, è chiaro che ereditano gli stessi problemi di sicurezza dei loro ben più seriosi colleghi. Non è una paranoia, se pensiamo che già nel 1999 la National Security Agency mise al bando i "Furby" dai propri uffici, (http://io9.gizmodo.com/the-nsa-once-banned-furbies-as-a-threat-to-national-sec-1526908210)perché riteneva che la loro capacità di migliorare la pronuncia col tempo dipendesse da un sistema di registrazione che avrebbe potuto inviare chissà dove delle informazioni riservate.

All'epoca, in effetti, si trattava di un azzardo, ma con le tecnologie attuali e l'uso di Internet è una possibilità tutt'altro che remota. Al punto che, proprio quest'anno, è partita una denuncia alla Federal Trade Commission da parte di un gruppo di associazioni internazionali contro due prodotti destinati ai bambini: My Friend Cayla e I-Que Intelligent Robot, della Genesis Toys. Il problema è essenzialmente uno: in quanto "smart", questi giocattoli si collegano alla Rete, e con questa scambiano dati.

Facciamo un esempio. Un nostro comando vocale, impartito alla bambola di turno, passa per un microfono, da qui viene digitalizzato e inviato a un server collocato chissà dove nel mondo. Ora, se il comando è "ridi", in fondo, non c'è problema. Il server interpreta il comando e fa in modo che la bambola crepi dalle risate. Ma questo raffinato sistema di riconoscimento, in realtà, è sviluppato per interpretare comandi ben più complessi, come quelli che impartiamo di solito a Siri di Apple, Google Now o Cortana di Microsoft, per intenderci. Comandi quali "Canta Without You di Mariah Carey". Già da una frase come questa, il server che costituisce, di fatto, il cervello della bambola, può ricavare una preferenza per questa canzone di questa specifica cantante. Non male, se poi questa informazione viene venduta ai distributori di musica digitale, no?

Mirko Gatto, CEO di Yarix, azienda di cybersecurity del colosso Var Group, è di questa idea: "*Molti smart toys memorizzano le comunicazioni nei server centrali e questo pone grossi problemi di privacy*".

Forse una preferenza musicale come quella descritta, senza riferimenti precisi a una persona, non è poi così preoccupante. Ma se il giocattolo è dotato pure di un ricevitore GPS? Molti smart toys ne incorporano uno per calcolare dei tragitti da percorrere in perfetta autonomia. E se la posizione fosse associata a una preferenza, l'**informazione per il distributore di musica digitale diventerebbe ancora più appetitosa.**

"Per questo si deve avere pazienza e mettersi a leggere la condizioni di privacy allegate al giocattolo smart: solo così sapremo dove andranno a finire i nostri preziosi dati", continua Gatto.

Adesso mettiamo che la nostra ipotetica bambola, così brava a parlare e a spostarsi in autonomia, abbia anche la capacità di "osservarci". Magari per capire se le muoviamo il viso davanti, o se si è al buio ed è ora di fare la nanna. Si tratta di funzioni tutto sommato ingenue, espletate con disinvoltura da una telecamerina interna. Che, tuttavia, potrebbe essere collegata anche al web affinché un genitore possa "spiare" il bambino mentre gioca, comodamente da un browser. Una vera e propria panacea per accontentare bimbi esigenti e tutori ansiogeni, ma che dal punto di vista della privacy può tornare indietro come un boomerang.

Il CEO di Yarix conferma: "*Per un hacker introdursi in sistemi del genere è semplice e, una volta preso il controllo di una telecamera, ha modo di vedere tutto ciò che il giocattolo punta: i rischi per la privacy e la sicurezza sono enormi".*

Ecco dunque perché, se a Natale si è ricevuto in dono uno di questi favolosi giocattoli, è comunque bene prendere qualche precauzione, lettura delle condizioni di privacy a parte.

Innanzitutto, accertarsi di quanti dati si passano effettivamente allo smart toy. Se sono tanti, verificare che il dispositivo abbia qualche sistema di protezione, magari via password, e attivarlo. E ovviamente assicurarsi che la password della rete wi-fi utilizzata sia degna di questo nome, e che vi sia una password sicura anche per l'accesso al router (di solito è"admin"…). Infine, l'ultimo consiglio ce lo fornisce proprio Mirko Gatto, particolarmente preoccupato dai rischi derivanti dall'uso di questi giocattoli: "*Può sembrare banale, ma cerchiamo di usarli il meno possibile"*. Al momento, in Italia non sono ancora commercializzati, se non tramite canali d'importazione illegali, ma visto che l'arrivo è solo questione di tempo, vale la pena farsi trovare preparati.