Un piccolo vademecum aiuta a mantenere calma ed efficienza operativa

Come vivere tranquilli con i nostri apparecchi elettronici

di Marco Manenti

Siamo circondati da apparecchi elettronici con i quali quotidianamente interagiamo, oggetti a cui magari affidiamo pezzetti della nostra vita, confessiamo nostri segreti, oppure in cui confidiamo per migliorare la nostra sicurezza.
Giorno dopo giorno, abbiamo sostituito apparecchiature meccaniche ed elettromeccaniche con apparecchiature elettroniche. È ormai cosa dovuta saper programmare il forno, il termostato, il televisore. Il telefono è diventato talmente evoluto da poter soppiantare un computer, l'antifurto ci permette di verificare – ovunque noi siamo – lo stato della nostra abitazione. Strumenti, questi, chiamati "intelligenti".
Nutrendo una forte passione per l'informatica e l'elettronica quando sento parlare di "computer intelligenti" o "robot intelligenti" sorrido. Non esiste – a livello pratico e diffuso – nulla di intelligente. Il processore è per sua natura *stupido*. L'unica intelligenza è (o dovrebbe essere) quella di chi lo ha programmato. Ma non è sempre così. Capita sempre più frequentemente, vuoi per budget ridotti o per incosciente pressapochismo, che la programmazione sia affrettata ed incompleta. Ne conseguono problemi di funzionamento e di sicurezza nell'utilizzo dei nostri apparecchi elettronici. Nel 1999 una sonda della Nasa (Mars Climate Orbiter) si è schiantata perché programmata a ricevere dati con il sistema metrico decimale, ma da Terra i dati sono stati inviati con il sistema imperiale.

Marco Manenti

I maggiori rischi derivanti da una inadeguata programmazione riguardano la sicurezza e la privacy.
Per quanto concerne la Sicurezza vanno smentiti alcuni pregiudizi.
Qualunque apparecchio elettronico è violabile, pertanto è sbagliato pensare "a chi può interessare il mio" per sentirsi sicuri.
Non esistono sistemi o software in grado di proteggere "al 100%" tali apparecchi.
Spesso però è sufficiente affidarsi al buon senso per poter ottenere buoni livelli di sicurezza. Qualche esempio:

- non utilizzare password facili (*123456* è usata da migliaia di persone, *qwerty* o *pippo* seguono a ruota), occorre invece sforzarsi di scegliere una password che contenga almeno una maiuscola ed un numero. Solitamente un buon suggerimento è quello di partire scegliendo una frase di una poesia ed utilizzare le iniziali – o le finali – di ogni parola per comporre la password, aggiungendo una inziale ed un numero (*Sempre Caro Mi Fu Quest'Ermo Colle* diventa *Scmfqec7*);
- cambiare la password *di default* (ovvero quella proposta in fase di installazione) di qualunque oggetto andiamo ad installare;
- cambiare la password con frequenza breve per i dispositivi o i siti più importanti;
- non collegare i dispositivi ad internet se non si hanno adeguate competenze tecniche;
- aggiornare il prima possibile il firmware (il software che pilota l'apparecchiatura);
- non installare software di cui non si conosca la provenienza;
- non premere pulsanti a caso soprattutto se state navigando su una pagina internet zeppa di pubblicità.

Cosa si rischia? Spesso molto. Qualche semplice esempio:

- Avere l'accesso al vostro modem/router ADSL significa ad esempio potervi installare un programma appositamente ideato per farvi credere di visitare il sito della vostra banca, mentre invece siete stati artificiosamente instradati verso un sito fasullo (*DNS Hijacking*). Nessun antivirus lo saprebbe mai, il *malware* non è installato sul PC.
- Applicazioni sconosciute possono rendere il vostro smartphone un "ripetitore" di tutto quanto transita dal terminale (password, codici segreti) o renderlo un perfetto registratore ambientale.
- Collegare una webcam ad internet senza prestare attenzione comporta la possibilità di essere osservati da chiunque (www.insecam.org/cam/bycountry/IT/) .
- Software non aggiornato porta addirittura ad esempi di *Wireless Carjackers*: pochi mesi fa è stata dimostrata la possibilità di prendere il controllo (freni, acceleratore, motore) di vetture Chrysler, Dodge e Jeep (ma neppure BMW, GM e altre marche ne sono uscite a testa alta).
- Con la domotica – ad esempio – possiamo da ogni parte del mondo pilotare il nostro sistema di climatizzazione, aprire e chiudere le imposte, le porte, o le finestre, avviare lavatrici, inserire e disinserire antifurti. Immaginate cosa potrebbe fare chiunque avesse il controllo del sistema. Purtroppo un sistema informatico spesso è progettato, costruito o installato senza tener conto della sicurezza. Recenti studi (es. Hewlett-Packard *How safe are home security systems?*) dimostrano con quanta superficialità viene gestita la sicurezza in ambito domotico.

Secondo una ricerca di Forbes nel 2015 saranno connessi ad internet circa 4,9 miliardi di dispositivi elettronici. Per il 2020 si stimano 26 miliardi di oggetti connessi. Non solo computer o smartphone, ma anche autovetture, orologi, termostati, frigoriferi, antifurti – insomma qualunque dispositivo moderno – possono o potranno a breve essere collegati alla Rete. Si chiama *Internet delle cose* (IoT – Internet of Things) e indica la possibilità che un oggetto venga collegato ad internet.

Se non prendiamo coscienza di dover dedicare maggiore attenzione alla sicurezza, quanti dispositivi interconnessi saranno compromessi? Come dobbiamo porci a proposito della sicurezza? Sicuramente dobbiamo prendere per buono questo principio: nulla è cambiato rispetto al passato. Come un tempo, più vogliamo essere *protetti* più il sistema dovrà essere *inviolabile*. Se questo discorso valeva per la catena della bicicletta, oggi vale per l'elettronica. Crittografia robusta come l'acciaio del lucchetto per esempio.

L'unica cosa che è cambiata è la percezione di questa sicurezza. Una volta potevamo valutarla dallo spessore della catena, ora dobbiamo fidarci ciecamente di uno specialista che possa consigliarci nell'acquisto, nell'installazione e nella – obbligatoria – manutenzione. E che poi ci segua negli aggiornamenti, come se non ne avessimo già a sufficienza di quelli di Entratel.

Marco Manenti
Dottore Commercialista