L'INTERVISTA MARK GASSON

E se mi si ammala il pace-maker?

Apparecchi medicali sotto attacco degli hacker? Fantascienza, ma non troppo

Nella fabbricazione di qualunque manufatto bisogna sempre ricordare una regola: più l'oggetto ha una struttura complessa, più diventa fragile e soggetto a problemi o malfunzionamenti. Basta un esempio semplice per capirlo: una palla di legno non si rompe cadendo per terra, mentre il modellino di una nave, fatto con lo stesso legno, si frantuma in mille pezzi. Purtroppo la regola vale anche per gli oggetti elettronici. Nessuno, acquistando un telefono cellulare di primissima generazione, avrebbe pensato alla possibilità che un hacker potesse attaccarlo mentre era impegnato in una conversazione con la fidanzata, così come ancora oggi facciamo fatica a pensare che un virus informatico possa entrare nel nostro frigorifero. Tuttavia ora molti smartphone dispongono di un programma antivirus preinstallato: una risposta efficace a una minaccia reale. E non è lontano il giorno in cui anche il nostro frigo, nel frattempo collegato a Internet, diventerà vulnerabile. Ora, se il frigorifero sembra forse un esempio eccessivo e ancora lontano dalla realtà, lo stesso non si può dire per i dispositivi elettronici salvavita, già ampiamente utilizzati per tutelare la salute di milioni di persone. Complicati, fragili e potenzialmente attaccabili.

PAGINA DI
ALESSIO PALMERO APROSIO

BATTICUORE Mark Gasson, sopra, si è impiantato un chip e poi lo ha infettato con un virus informatico. *(Foto Key)*

I moderni pace-maker dispongono già di un controllo remoto che permette ai medici dell'ospedale di configurare e monitorare i parametri vitali del paziente grazie a un collegamento wireless. Che cosa può succederebbe allora se un malintenzionato riuscisse a installare un virus informatico nel pace-maker? È quello che si è chiesto Mark Gasson, ricercatore presso l'Università di Reading, in Inghilterra, che nel marzo 2009 si è impiantato un chip di identificazione (analogo a quello utilizzato per gli animali domestici) e un anno dopo, nel maggio scorso, ha letteralmente infettato lo stesso chip con un virus informatico. «I primi dispositivi di identificazione erano dei semplici trasmettitori che ripetevano nell'etere un unico numero», ci spiega Gasson. «Successivamente si sono evoluti a tal punto che ora possiamo pensarli come dei piccoli computer. I modelli più evoluti, come quello che ho impiantato io, possono immagazzinare dati e compiere semplici calcoli».

Un successo strabiliante

> Il pericolo non è da sottovalutare e gli operatori devono sin d'ora prenderlo sul serio

Come nell'esempio della palla di legno, man mano che cresce la complessità dell'oggetto diminuiscono la sicurezza e la stabilità. «Per dimostrare la potenzialità di un'infezione», continua il ricercatore, «abbiamo eseguito due esperimenti differenti. Nel primo l'infezione ha avuto inizio nel computer del laboratorio usato per configurare il chip: il virus, come ci aspettavamo, si è trasferito automaticamente al dispositivo impiantato. Nel secondo esperimento, invece, siamo partiti infettando il chip: appena il computer è stato collegato, il virus ha fatto il suo dovere trasferendovi il suo codice malevolo». Un successo strabiliante, quindi, che però conferma inconfutabilmente come il problema non sia da sottovalutare.

«Non è stata una bella sensazione»

Qualcuno si chiederà che cosa si provi a diventare vittima in prima persona di un virus informatico. Su questo punto Mark Gasson non si sbilancia: «L'infezione che ho subito è stata deliberata e controllata, non ho sentito alcun effetto sul mio corpo e l'intera operazione è stata controllata accuratamente, in particolare nel momento in cui il dispositivo, come previsto, ha smesso di funzionare. Tuttavia non è stata una bella sensazione tenere un oggetto estraneo non più funzionante all'interno del mio corpo. Un oggetto del quale, in teoria, avrei potuto perdere il controllo. Se la mia salute dipendesse da quel dispositivo, il problema sarebbe reale e la situazione si farebbe molto pericolosa».

Il contagio è impossibile. Per ora

Parlando di un possibile contagio, il ricercatore britannico butta acqua sul fuoco: «L'aspetto positivo dei virus informatici è che sono scritti e studiati per una singola tecnologia. Ad esempio l'infezione, se così si può chiamare, utilizzata per compromettere il chip che ho impiantato non sarebbe nemmeno lontanamente pericolosa per un pace-maker o più in generale per un dispositivo differente anche di poco dal mio. Lo stesso discorso vale per i generici virus informatici che attaccano il nostro computer e che non possono trasferirsi spontaneamente in un pace-maker, a meno che non siano stati appositamente studiati per quello scopo. Di certo, tuttavia, il pericolo non è da sottovalutare e gli operatori del settore potrebbero andare incontro a problemi potenzialmente molto seri se non dovessero attuare protocolli di sicurezza adatti alla situazione».

Al confine fra biologico ed elettronico

> Stiamo parlando in realtà dell'interazione tra la tecnologia e il corpo umano

Guardando un po' più in profondità nel futuro, potrebbe suscitare interesse e perfino preoccupazione il cosiddetto «salto di specie». L'influenza aviaria e quella suina, di cui i media hanno discusso ampiamente, sono esempi di trasferimenti di un organismo pericoloso da una specie all'altra. I virus informatici, dal canto loro, non sono altro che codice informatico ed è quindi tecnicamente impossibile che si trasferiscano nella componente biologica del corpo umano. Il contrario, invece, non comporta difficoltà di tipo tecnico. Basterebbe immaginare un batterio in cui sia stato impiantato un DNA appositamente studiato per spingerlo a comportarsi in un certo modo quando incontra un dispositivo di un certo tipo. Il fatto poi che si tratti di un organismo vivente gli permetterebbe di trasferirsi tra un corpo umano e l'altro con i sistemi di contagio standard (ad esempio uno starnuto), altrimenti impossibili nel caso di virus unicamente informatici. «Ma per ora è solo fantascienza», replica netto Gasson. «Quella di cui stiamo parlando nella realtà è l'interazione tra la tecnologia e il corpo umano, spesso al punto in cui il corpo sopravvive proprio grazie a questi dispositivi. I virus organici attaccano il corpo umano, quelli informatici attaccano la tecnologia. Qualunque forma di crossover, allo stato attuale della ricerca scientifica e tecnologica, è da escludere».

Si perdono anche i benefici

> La comunità scientifica è cosciente dei potenziali danni di un attacco informatico

Questa risposta ci riporta coi piedi per terra, escludendo però di fatto a priori un secondo utilizzo, questa volta benefico, di esseri biologici che possano interagire con i dispositivi elettronici. Immaginiamo infatti di aver impiantato nel nostro corpo un pace-maker. L'azienda produttrice, dopo qualche mese dalla messa in commercio, scopre un pesantissimo problema di sicurezza informatica all'interno del dispositivo. Se si trattasse di computer o telefoni cellulari, una delle azioni da compiere potrebbe essere quella di richiamare i pezzi difettosi per sostituirli con le nuove versioni più sicure. Non sarebbe però così semplice se il dispositivo elettronico fosse impiantato in un corpo umano: diventerebbe necessario richiamare i pazienti ed eseguire nuovamente un'operazione chirurgica che, nel caso del pace-maker, potrebbe causare seri problemi. Se però l'azienda fosse in grado di produrre un batterio capace di riparare il guasto direttamente all'interno del corpo, non ci sarebbe bisogno di operare di nuovo tutti i pazienti. «In realtà è plausibile che un organismo cellulare possa trasportare al suo interno specifiche catene di DNA che portino informazioni verso un elemento tecnologico», ammette Gasson. «Ma sarebbe estremamente complesso nella realizzazione pratica ed è difficile pensare a come potrebbe rivelarsi utile. Ovviamente, se così fosse, la risposta alla questione discussa in precedenza sarebbe positiva, ma non riesco a immaginare che possa davvero diventare realtà».

La privacy è a rischio?

Se l'esperimento di Gasson svoltosi nei mesi scorsi può far pensare a un problema completamente nuovo di cui ancora nessuno si è occupato, in realtà la comunità scientifica è pienamente cosciente dei danni che un attacco informatico può causare alla vita di persone con dispositivi medici. Alcuni studi del 2008 condotti dal Medical Device Security Center, con ricercatori provenienti da vari istituti sparsi per tutti gli Stati Uniti, hanno preso in considerazione la tecnologia attuale, scoprendone pregi e difetti ma soprattutto individuando un secondo problema legato ai chip di identificazione: la privacy. La tecnologia utile per penetrare nelle reti wireless è ormai una realtà alla portata di tutti, cosicché un banale personal computer può intercettare i segnali trasmessi da chip, defibrillatori e impianti di vario tipo, per immagazzinare dati confidenziali come nome e cartella clinica di un paziente, utilizzabili poi da aziende o assicurazioni per scopi moralmente (e legalmente) discutibili.

Impianti utili ma non indispensabili

> I pericoli tanto temuti sono per adesso ancora lontani dal diventare un rischio reale

«A questo proposito», conclude Gasson, «non è impensabile che in futuro sempre più persone scelgano di farsi impiantare dispositivi o chip, se questo portasse loro benefici anche non strettamente indispensabili». Ma è già successo nella storia della medicina? Gasson ritiene di sì: «La chirurgia plastica, per esempio, è nata come soluzione ai difetti derivanti dalle operazioni chirurgiche e in breve si è trasformata in una questione squisitamente cosmetica». Se davvero l'elettronica entrerà massicciamente nei nostri corpi, l'attenzione alla sicurezza diventerà fondamentale, perché ciascuno di noi potrà potenzialmente essere attaccato mentre passeggia per strada e diventare preda di spammer di nuova generazione, avidi di informazioni e pronti a raccogliere i nostri dati personali. Magari (perché no?) per modificarli innestando malattie di cui non soffriamo, per spingerci così a comprare farmaci di cui non abbiamo bisogno.
Concludiamo però con una nota positiva: tutti gli studi sono concordi nell'affermare che i pericoli tanto temuti, in particolare quelli che prevedono un'interferenza attiva nel ruolo del dispositivo impiantato, sono per adesso ancora lontani dal diventare un rischio reale per la salute. Quindi, applicando le stesse precauzioni utilizzate per la chirurgia estetica, il consiglio è sempre lo stesso: informarsi adeguatamente, valutare il rapporto tra rischi e benefici, e solo allora fare una scelta. Sperando che sia la migliore.

LA QUESTIONE

È possibile infettare con un virus informatico un dispositivo elettronico salvavita, tipo pace-maker?
Per capirlo, il ricercatore Mark Gasson si è impiantato un chip di identificazione (analogo a quello utilizzato per gli animali domestici) e un anno dopo, nel maggio scorso, ha letteralmente infettato lo stesso chip con un virus informatico per vedere cosa succedeva.
Gasson e i suoi colleghi, ricercatori dell'Università di Reading, in Inghilterra, hanno eseguito due esperimenti:
Nel primo esperimento l'infezione ha avuto inizio nel computer del laboratorio usato per configurare il chip: il virus, come ci si aspettava, si è trasferito automaticamente al dispositivo impiantato.
– Nel secondo esperimento, invece, è stato infettato il chip: appena il computer è stato collegato, il virus ha fatto il suo dovere trasferendovi il suo codice malevolo.
«Tenere un oggetto estraneo non più funzionante all'interno del mio corpo – ha spiegato Gasson – non è una bella sensazione. Un oggetto del quale, in teoria, avrei potuto perdere il controllo. Se la mia salute dipendesse da quel dispositivo, il problema sarebbe reale e la situazione si farebbe molto pericolosa».