SE L'ASSICURAZIONE È A RISCHIO

L'INFORMAZIONE È POTERE E LE BANCHE DATI SONO L'OGGETTO DEL DESIDERIO DI MOLTI HACKER. LA VULNERABILITÀ DEI DISPOSITIVI RAPPRESENTA UNA FACILE CHIAVE D'ACCESSO DELLE RETI. DALL'HOME INSURANCE ALLE AGENZIE, DALLE SMART BOX AL MOBILE, LE MINACCE PER LE COMPAGNIE NECESSITANO DI ESSERE BEN COMPRESE

Abbattere le distanze con il web è un vantaggio per tutti, anche per chi ora può dedicarsi alle frodi con la garanzia dell'anonimato e può contare su un mercato della ricettazione che fonda le sue radici nella parte oscura del web, il cosiddetto *dark web*. Buona redditività e scarsa probabilità di essere scoperti hanno fatto esplodere il volume degli attacchi cyber in tutti i settori. Dell'industry assicurativa ciò che fa più gola è la grande quantità di informazioni sensibili detenute dalle compagnie: "ci confrontiamo con un settore che gestisce un patrimonio informativo appetibile per molti, compresi gruppi di criminali informatici, governi stranieri che vogliono acquisire informazioni riservate e attivisti", precisa **Pierluigi Paganini**, membro dell'**Enisa**, l'agenzia dell'Ue per la sicurezza delle reti e dell'informazione, e del gruppo di lavoro *Cyber G7 Summit 2017*.

I DATI, L'OBIETTIVO PIÙ AMBITO

La principale minaccia è quindi la violazione dei dati: "Tra i metodi di attacco adottati dai pirati del web, lo *spear phishing* è particolarmente insidioso: è una tecnica in base alla quale la vittima riceve un messaggio specificamente composto perché risulti di suo interesse e la invogli all'apertura di un allegato o di un link malevolo. Può avvenire che l'hacker sia a conoscenza di una particolare informazione relativa alla compagnia e invii una mail con oggetto che richiami tale informazione in modo da trarre in inganno la vittima". Si tratta di rischi trasversali a tutte le imprese, ma che diventano particolarmente densi di conseguenze se coinvolgono aziende che detengono milioni di dati sensibili relativi ai propri clienti: "al momento non ci sono notizie di attacchi specifici andati a buon fine nel settore *Insurance* in Italia. A livello mondiale ha fatto clamore il *data breach* subito da **Anthem**, il secondo maggior fornitore Usa di assicurazione sanitaria, che nel 2015 ha denunciato la compromissione dei suoi *data base* con il furto di dati di decine di milioni di utenti, inclusi i profili completi dei clienti. Ma non facciamoci trarre in inganno dal fatto che si tratti di un caso, per ora, unico. Negli ultimi mesi gli attacchi si sono moltiplicati e sono stati rubati miliardi di credenziali che sono ora disponibili nel dark web per i criminali intenzionati a realizzare furti di identità o frodi finanziarie".

Conoscere la data di scadenza di una polizza può dare luogo a tentativi di *phishing* mirato, con e-mail che propongono una promozione sul rinnovo se si forniscono determinati dati personali, o un omaggio offerto a un *prezzo speciale* registrandosi a un certo sito. "Nel dark web esistono *black market* specializzati dove si vendono lotti compositi di migliaia di credenziali ai migliori offerenti. Se poi ai dati della vittima si possono associare i

file dei documenti, come la carta di identità o la copia di bollette, l'hacker è in grado di impossessarsi dell'identità dell'ignaro cliente. In questo caso, chi subisce il data breach si troverà a far fronte al rischio reputazionale, ai danni economici diretti e indiretti, oltre al rischio di rivalsa degli interessati riguardo la mancata custodia dei dati o la mancata informazione sul furto".
Questi casi sono solo alcune delle *opportunità* a disposizione di chi si impossessa di tali archivi e, forse, anche le più *innocue*: "non possiamo trascurare – aggiunge Paganini – la possibilità che il furto avvenga su commissione o che i dati raccolti siano passati alla concorrenza. C'è poi l'utilità commerciale diretta: gli interessi di lettura, i beni posseduti, la tipologia di acquisti on line possono servire alle agenzie di pubblicità per profilare l'utenza. Oggi l'informazione è potere, commerciale ma anche decisionale. I dati sono i principali asset delle aziende".

PIÙ SICUREZZA PER I DEVICE TECNOLOGICI

Lo sviluppo relativamente recente di IoT è accolto da un approccio entusiastico che spesso induce a trascurare gli elevati rischi di vulnerabilità: "il paradigma IoT riferisce oggetti intelligenti esposti in rete che gestiscono una grande quantità di informazioni, allargando in maniera drammatica la nostra *superficie di attacco*. Molto spesso il livello di sicurezza implementato per questi dispositivi non è sufficiente a garantire una protezione dalle principali minacce cibernetiche, con drammatiche conseguenze. Modem, Dvr, camere si sicurezza e smartphone sono potenziali obiettivi degli hacker", spiega Paganini. Una grossa sfida, che coinvolge le assicurazioni non solo nell'offerta di polizze di tutela ma anche come utilizzatori di device e fornitori di strumenti digitali, è quindi la *Ict security* dei dispositivi e dei componenti. "Una smart box di una vettura, ad esempio, è un dispositivo intelligente sempre connesso che potrebbe essere obiettivo di attacchi. È accaduto nel 2015, quando due popolari hacker hanno dimostrato di poter prendere il controllo di un veicolo in movimento. Tutto ciò è allarmante se pensiamo che qualcuno in un luogo del mondo può controllare una macchina in qualunque altro posto mettendo a rischio la sicurezza di ignare persone".

NON SOLO OPPORTUNITÀ DI BUSINESS

Secondo Paganini, il duplice coinvolgimento delle imprese assicurative sul tema del rischio digitale presenta una certa forma di ambiguità: "da un lato la compagnie guardano alla *cyber insurance* come a un'interessante opportunità di business, dall'altro il livello di consapevolezza della minaccia è ancora basso. È come dire di vendere polizze per il furto delle auto mentre si lascia il proprio veicolo esposto ai ladri. L'anello debole della sicurezza è l'individuo, per cui è necessario investire nella formazione di tutte le funzioni aziendali per renderle consapevoli. Parlare di questi temi – conclude Paganini – cambia l'approccio verso gli strumenti informatici e aumenta l'attenzione di chi opera, può aiutare a ridurre il rischio di diventare una potenziale vittima. È necessario un cambio culturale, soprattutto per le reti agenziali. Ma da questo siamo ancora lontani". ***M.M.***