Virtual card, quanto mi costi

Sono sempre più frequenti le truffe informatiche a danno degli hotel che affidano ai portali il compito d'incassare i pagamenti

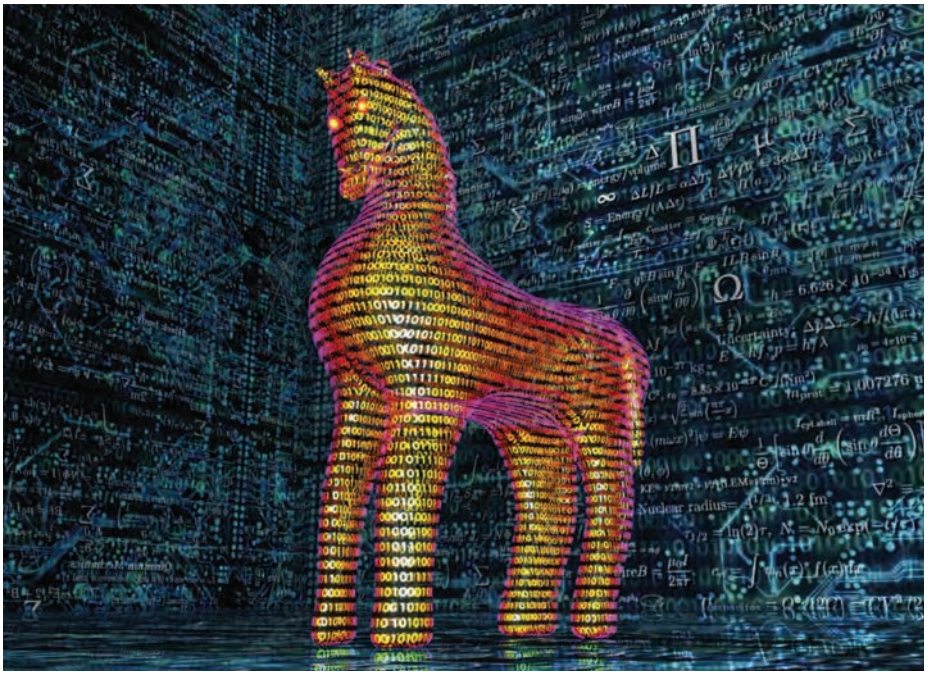
di Alessandro Massimo Nucara*

Sempre più spesso gli albergatori sono vittime di delitti realizzati mediante le carte di credito virtuali emesse dai portali di prenotazione, note anche come VCC (virtual credit card).
Non si tratta di una novità in senso assoluto. Né dell'unico tipo di attacco informatico che subiscono gli hotel. Ma negli ultimi tempi, le frodi in cui sono coinvolte le VCC hanno assunto dimensioni preoccupanti, sia per il numero di episodi rilevati sia per l'entità degli importi sottratti alle strutture, che in alcuni casi hanno raggiunto le centinaia di migliaia di euro.
Inoltre, non vanno sottovalutati i costi indiretti: tempo perso in dispute, danneggiamento della reputazione, perdita di clienti fedeli che hanno subito frodi. Insomma, il problema va ben oltre la singola transazione fraudolenta.
Come recita un antico proverbio, "praestat cautela, quam medela" (prevenire è meglio che curare). In altri termini, tutte le strutture dovrebbero prendere coscienza dei pericoli più diffusi e adottare le necessarie contromisure, auspicabilmente prima che tali aggressioni si verifichino.
Ed è per questo motivo che ne parliamo qui, anche traendo ispirazione dal contributo di imprenditori e consulenti del settore hospitality.**

LE FRODI PIÙ DIFFUSE

Anche se i reati che vengono perpetrati si basano su artifizi e raggiri in continua evoluzione, possono essere individuati degli schemi comuni.
Il trucco che sarebbe in teoria più facile da riconoscere (ma, ahimè, continua a mietere molte vittime) è quello in cui i malintenzionati riescono a farsi consegnare le chiavi di casa dagli stessi operatori. Il caso classico è quello dell'addetto al ricevimento che riceve una telefonata da qualcuno che si spaccia per manutentore del software (ad esempio, dichiara di essere un tecnico del channel manager che deve aggiornare il programma e comunica che in assenza di riscontro immediato verrà bloccata la possibilità di ricevere prenotazioni) e chiede l'accesso per poter effettuare un intervento da remoto. Sembra incredibile, ma non sono pochi coloro che "abboccano all'amo", anche a causa del fatto che la telefonata arriva di tardo pomeriggio o la sera, quando è più facile che non sia presente in azienda chi ha la competenza e l'autorità per opporsi all'inganno.
Questo tipo di intrusione è agevolata dal fatto che la teleassistenza è diventata la modalità abituale di intervento per gran parte delle aziende che forniscono software agli hotel.
Oggi entra in scena anche l'intelligenza artificiale generativa, che rende ancora più fragile il confine tra realtà e simulazione, consentendo di clonare voci e volti con una precisione tale da risultare indistinguibili dagli originali. Basta una manciata di secondi di audio o una semplice fotografia per generare un avatar parlante, capace di sostenere un dialogo in tempo reale con intonazione, pause e mimica credibili.
Questi strumenti sono alla portata di chiunque, economici e facili da usare, e stanno alimentando un nuovo fronte di truffe, in cui non serve più violare un sistema informatico, ma basta replicare l'identità di una persona per ingannare clienti o dipendenti. In questo scenario, la fiducia diventa un punto debole strut-

turale e la sicurezza non può più limitarsi alla protezione dei dati, ma deve estendersi alla tutela dell'identità stessa.
In altri casi, i criminali riescono a impossessarsi delle virtual card scavalcando gli addetti della struttura. A fare il lavoro sporco è un Trojan horse, cioè un malware che si presenta come un software legittimo e inganna l'utente, ottenendo subdolamente l'accesso al sistema informatico. Va peraltro detto che i cavalli di Troia non si diffondono autonomamente, ma vengono installati dall'utente stesso, spesso tramite download da siti non sicuri o aprendo allegati di e-mail.
Un ulteriore tipo di truffa viene realizzato mediante un messaggio, apparentemente proveniente dal portale, che viene spedito ai clienti che hanno prenotato, invitandoli a cliccare su un link, per effettuare il pagamento della camera o una verifica aggiuntiva della carta di credito.
Oltre a questo tipo di messaggio, che raggiunge il cliente via posta elettronica, si notano anche casi in cui l'ospite viene contattato tramite whatsapp.



Le truffe che vengono messe in atto sono di diverso tipo e in continua evoluzione

In questo scenario al cliente non viene chiesto il pagamento ma solo l'inserimento delle credenziali della carta di credito per motivi di verifica e per tenere attiva la prenotazione. Il canale è differente, ma l'obiettivo e le modalità non cambiano: ottenere i dati della carta di credito del cliente, presentando la richiesta come semplice procedura tecnica.
Viene spontaneo domandarsi come abbiano fatto i truffatori a entrare in possesso della lista delle prenotazioni, del prezzo concordato, degli indirizzi di posta elettronica e dei recapiti telefonici dei clienti. A che livello è avvenuto il data breach? Quale sistema è stato violato? Quello del portale, quello del channel manager, quello del property management system, quello dell'albergo?
C'è la tendenza a credere che l'hotel, ultimo anello della catena, finisca per essere il soggetto più esposto e più vulnerabile. Ma non è detto che sia sempre così. Ad esempio, sono stati segnalati casi in cui un gran numero di messaggi è stato inviato contemporaneamente tramite la extranet di un noto portale, che però non consente alla struttura di effettuare operazioni massive.
Quale che sia l'espediente utilizzato, il risultato è sempre lo stesso: l'hotel viene defraudato e, purtroppo, le speranze di rientrare in possesso del maltolto si riducono al lumicino.

ALCUNE PRECAUZIONI DA ADOTTARE

L'hotel può elevare sensibilmente l'efficacia delle proprie barriere di autodifesa, adottando alcune precauzioni. L'aggiornamento dei sistemi di sicurezza è un presupposto indispensabile. Si parte da:
- installare antivirus e antimalware, per rilevare e rimuovere virus, Trojan e altri software dannosi;
- mantenere il sistema operativo e i programmi aggiornati per chiudere eventuali falle di sicurezza.

Altrettanto importante è la sensibilizzazione dei collaboratori. Ma non basta invitare genericamente gli addetti a essere più attenti, bisogna fornire indicazioni specifiche su come farlo.
Ad esempio, all'interno della to-do list aziendale, non dovrebbero mancare alcuni accorgimenti operativi:
- sancire il divieto assoluto di comunicare le password a soggetti esterni e/o di consentire loro in alcun modo l'accesso ai sistemi aziendali;
- gestire con estrema cautela le richieste telefoniche provenienti da sconosciuti;
- raccomandare una sana prudenza a fronte di messaggi che potrebbero "incubare" un Trojan: non aprire allegati di e-mail sospette, verificare l'attendibilità del mittente prima di aprire allegati;
- prestare grande attenzione ai download: scaricare software solo da fonti affidabili;
- attivare uno user dedicato per ogni membro dello staff e definire per ciascun account le specifiche autorizzazioni, così

in caso di phishing sarà più facile individuare la falla e limitare le operazioni fruibili mediante l'account hackerato;
- aggiornare periodicamente le password dei portali e della webmail, tenendo presente che Excelsior2022* NON è una password sicura (una password sicura potrebbe essere 3Xc3lS10r$2025;X%);
- simulare tentativi di frode durante i meeting;
- mettere in pagamento le virtual card non appena possibile, per non lasciarle troppo a lungo alla mercè di eventuali truffatori;
- ricordare sempre che, a fronte di un dubbio, la richiesta del parere di un collega più esperto o del consulente aziendale non è sintomo di incompetenza ma indice di professionalità.

Si può anche valutare la possibilità di chiedere ai portali di versare le spettanze future dell'albergo mediante un bonifico, anziché mediante una carta di credito virtuale.

In genere, i portali non incoraggiano il passaggio al bonifico e sottolineano che questa scelta non è facilmente reversibile. Inoltre, gli alberghi che utilizzano tale sistema segnalano alcune complicazioni sul versante fiscale e amministrativo, connesse alla gestione dei cosiddetti "sospesi", in quanto di norma l'albergo riceve il bonifico dal portale alcuni giorni dopo la partenza del cliente.

Per quanto riguarda i costi, va ricordato che i portali applicano una commissione anche sui bonifici. Di norma è inferiore a quella pagata per incassare le carte di credito virtuali, ma è sempre bene informarsi e chiedere di mettere per iscritto le condizioni.

Gli argomenti trattati in questo articolo saranno ulteriormente approfonditi nel corso di un panel che si svolgerà nel pomeriggio del 12 novembre alla Stazione Leopolda di Firenze, nell'ambito della BTO 2025.

COSA FARE SE SI VIENE ATTACCATI

Una delle prime cose da fare se si teme di essere stati aggrediti da un malware è disconnettere il sistema: il computer infettato deve essere scollegato dalla rete il più rapidamente possibile per evitare danni peggiori.

Subito dopo, insieme ai propri partner tecnici (in primis, i fornitori del channel manager e del pms) e ai propri collaboratori occorre svolgere un'analisi accurata dell'accaduto, focalizzando l'attenzione sia sull'infrastruttura (hardware e software) sia sulle procedure, per individuare eventuali falle e adottare gli opportuni correttivi.

Ad esempio, per prevenire il rischio che la cosa possa ripetersi, può essere opportuno resettare o bloccare tutte le password, preferibilmente accedendo da un dispositivo diverso da quello utilizzato abitualmente.

In parallelo, occorre inoltre scrivere al portale, chiedendo un intervento tempestivo per tamponare le perdite e riparare il danno, e presentare una denuncia all'autorità competente, che di norma è la Polizia postale.

Non di rado i portali rispondono negando ogni responsabilità e affermando in modo dogmatico che l'hotel è stato vittima di phishing, diretta conseguenza del basso livello di sicurezza della struttura e delle procedure. Oppure si dimostrano poco reattivi, offrendo riscontri a dir poco evanescenti.

Non è detto che tale atteggiamenti debbano essere accettati supinamente. Alcuni hotel, disponendo di buoni argomenti per dimostrare che la responsabilità dell'accaduto sia estranea alla struttura ricettiva, hanno chiesto ai portali di reintegrare il maltolto e, in caso di risposta negativa, hanno intentato delle azioni legali.

PERCHÉ È MEGLIO FARE A MENO DELLE VCC

Tutto ciò premesso, non ci stancheremo mai di ricordare che, se si smette di affidare ai portali il compito di incassare quanto dovuto dai clienti, si elimina alla

radice buona parte dei rischi che abbiamo descritto.
Al riguardo, va anche sottolineato che le virtual credit card – che vengono apprezzate soprattutto per ragioni di comodità – oltre a creare i presupposti per molte truffe, presentano diverse controindicazioni, che possono risultare ancor più deleterie delle truffe stesse.
La prima conseguenza negativa è data dal fatto che l'hotel perde il controllo delle proprie tariffe. Affidando al portale il compito di incassare gli si affida, infatti, anche la facoltà di modificare i prezzi decisi dalla struttura.
Un classico esempio è il programma Booking Sponsored Benefit di Booking.com, in cui il portale riduce di sua iniziativa i prezzi, dichiarando di accollarsi il costo di una parte del soggiorno. A seguito dell'intervento dell'Antitrust, il portale si è dovuto impegnare ad assicurare che i prezzi applicati dalle strutture ricettive su canali di vendita online diversi da Booking.com non vengano presi in considerazione ai fini dell'applicazione del BSB.
Anche in questo caso, c'è più di un dubbio connesso alla gestione degli aspetti fiscali, sul quale è probabile che prima o poi l'Agenzia delle Entrate accenda un faro. Ad esempio: se il cliente ha pagato a Booking.com 85 euro, come si può chiedere all'albergo di rilasciare una ricevuta fiscale (rectius: documento commerciale) per il prezzo intero di 100 euro pubblicato in piattaforma? Se il cliente ha pagato 85 euro, potrà portare in detrazione l'importo intero? O chiedere un rimborso spese per l'importo intero?
Altro punto dolente riguarda le commissioni di transazione sulle VCC, che tendono a essere più alte rispetto a quelle dovute sulle "normali" carte utilizzate dal cliente. Ad esempio, anche se il cliente paga utilizzando una carta di debito retail emessa in Francia o in Germania (che di norma sconta commissioni più basse) la VCC emessa dal portale per pagare l'albergo sarà trattata come una carta di credito commercial emessa al di fuori dello spazio economico europeo, con l'applicazione di una commissione molto più alta.
Non va poi dimenticato che, se si affida al portale il compito di incassare il pagamento, sarà poi il portale a gestire le politiche di cancellazione e i rimborsi. Questo può portare a situazioni in cui l'hotel ha meno flessibilità nel gestire dispute o casi specifici o nel recuperare eventuali costi associati a cancellazioni tardive o "no-show". L'hotel potrebbe trovarsi a dover rimborsare un cliente anche se, in base alle proprie politiche, avrebbe avuto diritto a trattenere parte dell'importo.
Ultimo, ma non meno importante, quando il portale incassa direttamente dal cliente, l'hotel non riceve il pagamento immediatamente. Spesso, le online travel agencies versano i fondi agli hotel con cadenze prestabilite e solo dopo il check-out del cliente o la scadenza dei termini di cancellazione.
In definitiva: le virtual credit card possono apparire uno strumento comodo, perché ci consentono di alleggerire il peso di alcune incombenze. Ma – anche a prescindere da eventuali truffe – finiscono per costar caro all'albergo, determinando effetti indesiderati e dolorose sorprese.

**direttore generale di Federalberghi*

Se affidiamo al portale il compito di incassare il pagamento, sarà poi il portale a gestire le politiche di cancellazione e i rimborsi

** Ringraziamo per la collaborazione e gli spunti forniti: Daniele Barbetti, Vinicio Borsi, Marcello Carfora, Ermando Mennella, Raffael Mooswalder, Simone Puorto, Stefano Quarti, Andrea Romanelli, Nicola Seghi, Armando Travaglini, Stefano Visconti e Nicola Zoppi.