



2012 AUMENTANO LE MINACCE ALL'ONLINE BANKING?



**CAL CREDIT CARD
IMPLEMENTA IL SISTEMA
«SAFE SHOPPING»**



**I CONSIGLI PER
LA PROTEZIONE
DELLO SMARTPHONE**



**AGROALIMENTARE:
SEQUESTRATI
FORMAGGI E INSACCATI**



**SICUREZZA IN
MONTAGNA: ANCORA
RISCHIOVALANGHE**



CA Technologies ha annunciato che la società Cal Credit Card ha implementato il sistema "Safe Shopping" utilizzando la soluzione CA Arcot TransFort™ per emittenti. CA Arcot TransFort è un server di controllo degli accessi (ACS, Access Control Server) che fornisce, alle società che emettono e gestiscono carte di credito, servizi per la prevenzione delle frodi e l'autenticazione conformi al protocollo 3-D Secure. Il servizio è erogato sul modello cloud e garantisce diversi livelli di protezione e verifica dell'identità durante le transazioni effettuate in modalità shopping CNP (Cardholder-Not-Present). Il nuovo sistema Safe Shopping di Cal Credit Card conta 1,7 milioni di utenti e permette alla società di implementare

WWW.ILCORRIEREDELLASICUREZZA.IT

2012 AUMENTANO LE MINACCE ALL'ONLINE BANKING?

Il 2011 ha visto aumentare le minacce dirette al mondo dei servizi finanziari online, un trend che purtroppo si conferma costante per il 2012. Al fine di identificare quelle che saranno le principali sfide che i dipartimenti IT e le loro controparti business si troveranno a dover affrontare, Akamai ha commissionato uno studio all' IDC Financial Insights. In base ai rilevamenti della ricerca, Rich Bolstridge, Chief Strategist per i Servizi Finanziari di Akamai, ha stilato una lista di raccomandazioni utili per non lasciarsi cogliere impreparati.

ECCOLE DI SEGUITO:

1. I team responsabili dell' IT security devono garantire coerenza tra le strategie di sicurezza adottate e gli obiettivi di business, specialmente se, tra questi, figura lo sviluppo del canale di digital banking. Il coinvolgimento del team IT nella progettazione di nuovi prodotti e servizi va quindi previsto fin dai primissimi stadi, in modo particolare se ci si avvale di modalità d' interazione di ultima generazione quali social e mobile.
2. E' fondamentale essere pienamente consapevoli delle conseguenze di un malware mobile. Secondo IDC Financial Insight, le probabilità di attacco da parte dei cyber criminals, piuttosto basse nel 2011, potrebbero invece aumentare nell' anno in corso.
3. Le banche dovrebbero continuare – in alcuni casi, incominciare – a educare i consumatori, insegnando loro a riconoscere tentativi fraudolenti di accesso ai propri dati finanziari (dunque a identificare azioni di phishing o smishing). IDC ha rilevato che spesso i metodi utilizzati in passato sono stati ritenuti poco efficaci. Un training interattivo – attraverso cui la banca simula un attacco per accertarsi del fatto che i consumatori siano in grado di individuarne i segnali e agire di conseguenza - potrebbe essere una valida alternativa a quelli tradizionali.
4. Se i fornitori abituali di soluzioni di security non sono in grado di migliorare la robustezza del canale mobile, allora le singole organizzazioni dovrebbero valutare l' impiego di realtà specializzate, focalizzate esclusivamente sulle innovazioni in fatto di mobile security.
5. I dipartimenti IT dovrebbero coinvolgere maggiormente gli utenti business, al fine di ottenere sponsorizzazioni (e contributi finanziari) a sostegno di iniziative volte a migliorare la sicurezza del digital banking. Viceversa, gli utenti business dovrebbero invece valutare accuratamente il lancio di nuovi servizi o applicazioni prima che questi siano stati adeguatamente testati e approvati dal dipartimento IT.
6. Nel digital banking c'è ancora spazio per le innovazioni, a patto che queste siano sostenute da



soluzioni per la sicurezza altrettanto innovative. 7. Nel prossimo futuro, ci si aspetta un crescente numero di attacchi sia da PC sia da dispositivi mobili; le banche dovrebbero dunque pianificare di conseguenza le proprie strategie: è sempre meglio essere più preparati del dovuto piuttosto che essere colti alla sprovvista! Un futuro sicuro per la mobile finance Tra le minacce alla sicurezza emerse di recente, le più preoccupanti sono sicuramente quelle a danno del mobile. Gli utenti che usufruiscono dell' online banking da desktop, ben conoscono e comprendono le misure di sicurezza più basilari. Tali misure però, non hanno ancora un equivalente nel mondo mobile e quindi risultano sconosciute ai più. I servizi di mobile

finance, che prevedono un' applicazione nativa o un' applicazione ibrida in cui il browser è integrato all' interno di un' app, non offrono ancora misure di sicurezza altrettanto facilmente intuibili. La buona notizia è che, pur non essendo - ad oggi - così immediata, la mobile finance è destinata a divenire ancora più sicura dell' equivalente desktop. Questo perché, mentre il desktop browser è per sua natura più soggetto ad attacchi alla sicurezza, nel mondo mobile, gli sviluppatori hanno la possibilità di trarre vantaggio dall' applicazione nativa e controllare completamente la sicurezza dell' applicazione. I presupposti per un futuro più sicuro ci sono tutti.

I DATI E IL GRANDE FREDDO

I consigli di Kroll Ontrack per proteggere il nostro smartphone

Le avverse condizioni ambientali possono costituire un serio ostacolo all' uso dei dispositivi elettronici e in questi giorni, in particolare, stiamo sperimentando temperature piuttosto rigide rispetto alla media stagionale. Il freddo, ma più in generale gli sbalzi termici, possono danneggiare hard disk portatili, tablet, smartphone o fotocamere – che non dovrebbero mai essere utilizzati in presenza di temperature estreme - rendendo, di conseguenza, difficile o impossibile l' accesso ai dati memorizzati. “Quando per esempio ci si reca sulla neve per le vacanze invernali, oppure anche con il freddo particolarmente intenso di questi giorni, i nostri dispositivi possono manifestare malfunzionamenti. Pensiamo all' oggetto che più portiamo con noi: lo smartphone. La tecnologia impiegata nei touch screen si basa sui cristalli liquidi che possono smettere di funzionare correttamente in presenza di basse temperature. Ad esempio, alcuni test condotti sui cellulari con tecnologia

touch hanno dimostrato che essi iniziano a dare segni di malfunzionamento a partire da meno 10 gradi” commenta Paolo Salin, Country Director di Kroll Ontrack in Italia. Kroll Ontrack fornisce agli utenti semplici consigli che aiutano a conservare in buono stato il proprio smartphone e, in generale, prevengono la perdita dei dati memorizzati sui dispositivi elettronici: Lo smartphone deve essere sempre inserito in una custodia appropriata. Questo strumento è utile per isolare e proteggere il dispositivo non solo dagli urti ma anche dagli sbalzi di temperatura. Non esporre il cellulare troppo a lungo a temperature al di sotto delle zero. Se lo smartphone è stato troppo a lungo esposto a basse temperature non accenderlo immediatamente e non esporlo direttamente a fonti di calore come termosifoni, stufette o camini ma lasciare il dispositivo a temperatura ambiente per un po' di tempo, in modo tale che possa riacquistare gradualmente la temperatura circostante.

rapidamente il programma 3-D Secure per ridurre i rischi di frodi nelle transazioni CNP. "Abbiamo attuato il progetto Safe Shopping per permettere ai clienti di acquistare online con maggiore sicurezza. Le soluzioni di CA Technologies ci consentono di verificare in tempo reale l'identità del titolare della carta di credito, garantendo allo stesso tempo un elevato livello di soddisfazione all'utente finale", ha commentato Elaad Saar, responsabile del progetto alla Cal Credit Card. Per poter usufruire di questo nuovo servizio, i clienti devono registrarsi sul sito di Cal Credit Card o in occasione del primo acquisto online con Cal Credit Card. Al successivo acquisto online, viene loro chiesto di inserire i propri dati di accesso e la password di autenticazione personale che permette di verificare la titolarità della

carta. "Abbiamo scelto la soluzione di autenticazione avanzata di CA Technologies perché supporta il protocollo 3-D Secure che assicura a Cal Credit Card la conformità con gli standard di sicurezza dei circuiti delle carte di credito. In questo modo, i clienti si sentiranno più sicuri nell'eseguire le transazioni online," ha aggiunto Saar. "Siamo contentissimi che Cal Credit Card abbia scelto le nostre tecnologie di autenticazione avanzata per incrementare la sicurezza del suo sistema di pagamento per gli acquisti online. CA Advanced Authentication contribuisce a tranquillizzare i titolari, le società di gestione e le emittenti delle carte di credito, aggiungendo un ulteriore livello di sicurezza alle transazioni online," ha dichiarato Shai Onn, Country Manager di CA Technologies Israele.

WWW.ILCORRIEREDELLASICUREZZA.IT

SICUREZZA IN MONTAGNA: ANCORA RISCHIO VALANGHE

Il Corpo forestale dello Stato raccomanda di consultare i bollettini del Servizio Meteomont su www.meteomont.org

Resta alta l'attenzione del Corpo forestale dello Stato su tutte le zone montane ad alto rischio valanghe. In Piemonte il pericolo valanghe resta MARCATO. Tutto il settore è stato interessato da una nevicata di debole intensità. Le temperature negative della notte e la scarsa coesione del manto nevoso determina un aumento generale del rischio di distacchi spontanei o provocati con debole sovraccarico, specialmente alle quote superiori ai 1.800 metri. Si consiglia di evitare pendii ripidi e canali in particolare nelle ore più calde della giornata. Nella zona di confine

Sull'Appennino umbro-marchigiano il pericolo valanghe è MARCATO e il distacco è possibile con debole sovraccarico soprattutto sui pendii ripidi, a causa della scarsa coesione del manto nevoso. Il pericolo valanghe è MARCATO sui Grandi Massicci appenninici e in Abruzzo, dove nelle ultime ore si sono registrate deboli precipitazioni nevose che non hanno legato con lo strato sottostante. Pertanto il distacco di valanghe può essere spontaneo o provocato con debole sovraccarico. Si consiglia di evitare pendii ripidi e le attività fuoripista. Il pericolo valanghe scende a MODERATO in Valle d'Aosta, in Lombardia, in Veneto, sull'Appennino Settentrionale Tirrenico, in Emilia Romagna, sull'Appennino Calabro-Lucano e in Sicilia. Grazie al Meteomont, un servizio garantito dal Corpo forestale dello Stato e dal Comando delle Truppe Alpine, con la collaborazione del Servizio Meteorologico dell'Aeronautica Militare, gli abitanti della montagna, gli sciatori e i turisti, possono conoscere nel dettaglio le condizioni del manto nevoso e decidere se esistono o meno le condizioni di sicurezza per un'escursione.

I comandi stazione del Corpo forestale dello Stato sono impegnati proprio in queste ore nel rilevamento delle condizioni del tempo, dell'altezza della neve, dello stato della viabilità locale e negli interventi necessari per ripristinare la circolazione resa difficoltosa. Si può conoscere così l'evoluzione temporale e spaziale della perturbazione a carattere nevoso, della neve al suolo, delle difficoltà sulla circolazione stradale attraverso la pubblicazione costante dei dati elaborati e trasmessi in tempo reale sul sito www.meteomont.org, alla sezione "nevicata in atto". In particolare sono state segnalate forti difficoltà sulla viabilità stradale per presenza neve in diversi Comuni dell'Abruzzo della Toscana e dell'Emilia Romagna.

Si consiglia a tutti di consultare quotidianamente i bollettini meteonivologici pubblicati sul sito www.meteomont.org o chiamare al numero di emergenza ambientale 1515 del Corpo forestale dello Stato.



del Trentino Alto Adige il pericolo valanghe resta MARCATO. Il settore delle Alpi Breonie, Aurine - Pusteresi, nella notte è stato interessato da una nevicata di media intensità. La neve fresca non si è consolidata con lo strato preesistente, pertanto il distacco è possibile già con debole sovraccarico, soprattutto sui pendii ripidi oltre i 1.800 metri di quota. Con il rialzo diurno delle temperature e l'irraggiamento solare sarà possibile una ripresa dell'attività valanghiva spontanea. Nel resto del settore il pericolo valanghe è MODERATO e la tendenza generale del pericolo è in aumento. Nella zona di confine del Friuli Venezia Giulia il grado di pericolo è MARCATO in particolare su Alpi e Prealpi Carniche Occidentali e Giulie, mentre il pericolo è MODERATO su Alpi e Prealpi Carniche Orientali e Prealpi Giulie. Considerate le caratteristiche del manto nevoso e le precipitazioni che hanno interessato tutta la zona, il distacco sarà spontaneo o provocato già con debole sovraccarico.

SICUREZZA AGROALIMENTARE:

SEQUESTRATI FORMAGGI E INSACCATI

Quattro denunce per i reati di frode nell'esercizio del commercio e contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti

Formaggi e insaccati spogliati delle etichette originali e privati della tracciabilità, messi in vendita con false denominazioni e spacciati per prodotti alimentari a Denominazione di Origine Protetta (DOP) o a Indicazione Geografica Protetta. È quanto scoperto a Brescia dal Nucleo Investigativo Provinciale di Polizia Ambientale e Forestale (NIPAF) del Corpo forestale dello Stato che opera nella provincia lombarda, durante controlli effettuati nell'ambito della tradizionale fiera



di San Faustino, dove nella giornata di mercoledì sono confluiti circa 600 espositori provenienti da tutta Italia. Formaggi palesemente contraffatti che evocavano le DOP "Pecorino Toscano" e "Pecorino Sardo" e falso "Speck Altoadige" IGP. Quattro quintali di formaggio ovino e oltre 20 chilogrammi di speck sono finiti sotto sequestro. I quattro titolari degli altrettanti punti vendita ambulanti controllati sono stati denunciati alla Procura della Repubblica di Brescia per i reati di frode nell'esercizio del commercio e contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari, reato quest'ultimo che prevede la reclusione fino a due anni e una multa fino a 20.000 euro. Contestualmente sono state emesse sanzioni amministrative per oltre 16mila euro. In un caso è stato addirittura accertato che il formaggio ovino venduto come "Pecorino Sardo" DOP era in realtà un prodotto di origine tedesca. Rimane alta l'attenzione del Corpo forestale dello Stato su tali pratiche fraudolente che minano il prezioso patrimonio enogastronomico italiano e ingannano i consumatori che talvolta, senza saperlo, si trovano ad usufruire di prodotti di dubbia provenienza.

Con l'analisi dei media

la tua rassegna stampa
può dirti di più...

**Quanto si è parlato
di te. E chi
ne ha parlato**

**Com'è percepita
l'immagine
della tua azienda**

**Quanti lettori
e ascoltatori
sono stati raggiunti**

**L'efficacia
dei tuoi
Key Message**

**Qual è il valore
economico
della tua
comunicazione**

**Quanto lo spazio
dedicato ai
vertici aziendali**

**... e tante altre
cose che puoi
chiederci allo:**

06-35.40.80.1

datalab@analisiimedia.it

