Sicurezza e Internet I punti deboli e i consigli per evitare i blackout dei siti e della posta elettronica

Incendi, guasti, hacker: i buchi della Rete

Le preoccupazioni dopo il caso Aruba. Gli esperti: rischi seri se non si investe

MILANO — Per l'economia digitale è stata una settimana disastrosa: prima un guasto ai server di Amazon che ha causato notevoli disagi anche ad alcuni social network come Foursquare, Quora e Reddit.

Poi, sempre negli Usa, è stata la volta dei server della Sony attaccati da hacker che hanno avuto accesso a dettagli personali di 77 milioni di utenti. «Infortunio» pagato subito anche in Borsa dove le azioni sono scese del 5% e sul quale vuole indagare anche una sottocommissione della Camera dei Rappresentanti.

Il cyber-poliziotto

«La tecnologia ci spinge a portare tutti i dati sui server remoti. Ma questi vanno duplicati per non perderli»

Nella notte tra giovedì e venerdì poi è toccato all'Italia che, a causa di un incendio nella sede di Arezzo del provider Aruba, ha subito un blackout durato alcune ore per siti e email gestiti dal primo operatore italiano di web hosting.

Fino ad oggi avevamo in qualche maniera accettato che la nostra carta di credito e la nostra privacy non fossero del tutto al sicuro sul Web. Ma quello che accomuna gli eventi di questa settimana è la matrice sistemica, strutturale, del problema. Non è più solo argomento che interessa i cybernauti, i *nerd* o i consumatori. Il passaggio dal furto delle carte di credito ad Aruba è importante. Abbiamo scoperto che la Rete, il luogo «virtuale» per eccellenza può prendere fuoco. Letteralmente.

«Per descrivere eventi di questa portata dovremmo risalire al 2002 — ricorda Feliciano Intini, *chief security officer* di Microsoft — ma si trattava comunque di disastri causati da virus e comunque che toccavano le aziende».

Come quando l'esondazione di un fiume tra la Lombardia e il Piemonte, un fatto rimasto nel segreto fino ad oggi, aveva allagato fisicamente i server di una delle principali banche italiane. Ma anche in quel caso era stato un problema aziendale. Aruba dà invece la misura del cambio di passo. Ora sul Web ci siamo tutti.

È un fenomeno mondiale che crescerà sempre di più con il *cloud computing*, in sostanza la nuova gallina dalle uova d'oro, l'esternalizzazione dei dati strategici delle aziende su server posti chissà dove. Per capire quanto la questione sia nuova bisogna ricordare che Internet, in quanto infrastruttura virtuale, aveva finora retto anche all'11 settembre e al terremoto in Giappone. Anche durante i sanguinosi giorni della rivolta egiziana la Rete era stata tolta in maniera più canonica: gli operatori mobili come Vodafone erano stati obbligati dall'esercito allo *switch off*.

«La tecnologia ci sta spingendo a portare tutti dati sui server remoti grazie alla velocità della Rete e alle necessità della mobilità» spiega Gigi Carbone della PolPost. Prima si perdeva l'hard disk, oggi può scomparire una porzione di storia. «I server vengono replicati — conclude Carbone — il rischio potrebbe essere in una disfunzione sull'aggiornamento». Chiaro. Dipende da chi offre il *back up* dei dati. Le leggende metropolitane vogliono le *web farm* in posti isolati come la Siberia.

È famosa la grotta della Seconda Guerra Mondiale in Svezia dove sono fisicamente i server di Wikileaks. Dove si trovino i server delle maggiori società mondiali esattamente non lo sa nessuno. Gruppi come Google e Amazon considerano queste informazioni strategiche. Ma nella realtà le cose sono meno misteriose.

Per esempio le società italiane che si avvalgono dei servizi di *cloud* della Microsoft sanno che i propri dati vengono replicati nei server a Dublino e Amsterdam.

«Sono in territorio europeo per questioni legali» spiega Intini. Ma non tutti rispettano le regole.

«Chi fa sicurezza ha una serie di processi da manuale per difendersi. La paranoia paga. Ma metterla poi in campo ha un costo» conclude. La regola aurea rimane duplicare e sincronizzare regolarmente. Ma non solo. Ad Aruba per esempio l'errore è stato mettere le batterie troppo vicine ai server.

«Sono poco ottimista sulla sicurezza dei dati in Italia — confessa Intini — perché le aziende hanno investito solo quando è successo qualcosa di serio».

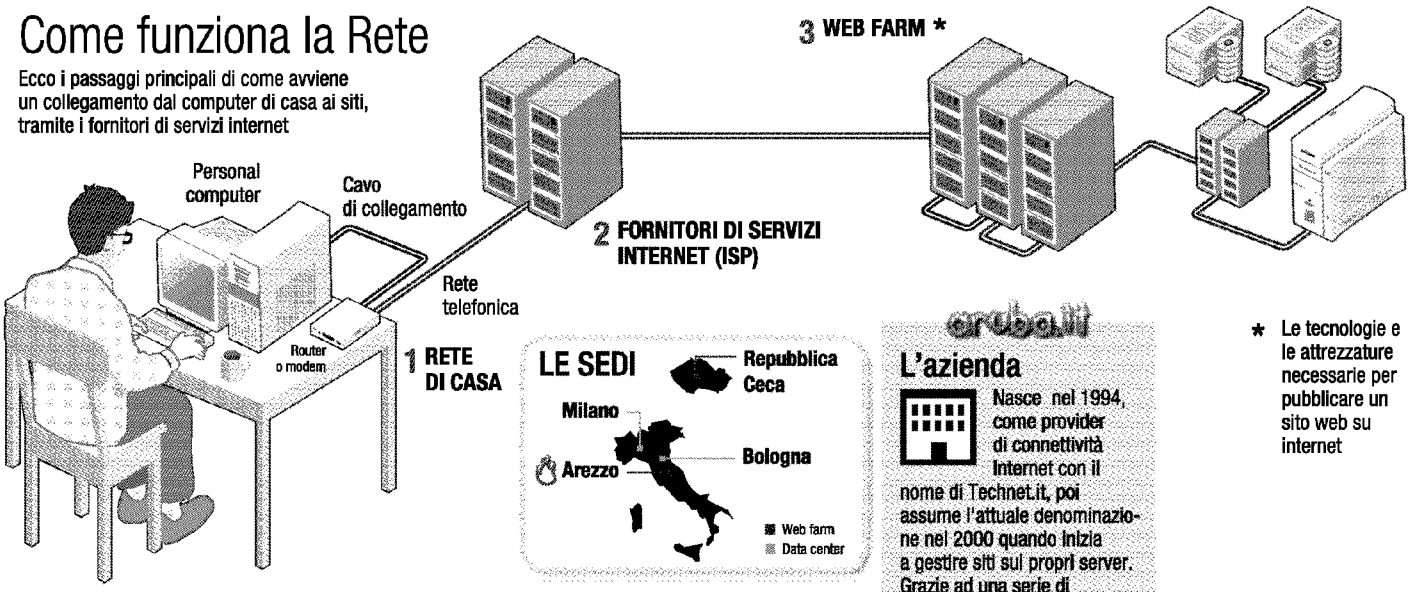
Alessio Ribaudo
Massimo Sideri

Gli interventi **dopo il rogo**

Ad Arezzo, i tecnici portano via il materiale danneggiato dall'incendio sprigionatosi all'interno degli armadi batterie a servizio dei sistemi Ups di Aruba (Ansa / Falsetti)

Come funziona la Rete

Ecco i passaggi principali di come avviene un collegamento dal computer di casa ai siti, tramite i fornitori di servizi internet



aruba.it

L'azienda

Nasce nel 1994, come provider di connettività Internet con il nome di Technet.it, poi assume l'attuale denominazione nel 2000 quando inizia a gestire siti sui propri server. Grazie ad una serie di acquisizioni oggi il gruppo è attivo con **14 marchi nel settore dell'hosting e della gestione dei domini**, ovvero degli indirizzi Internet dei siti web

Cosa fa

La web farm ospita sui suoi server, provvedendo a connetterli a Internet, **più di 1,25 milioni di siti web** e gestisce più di **1,65 milioni di domini registrati e 5 milioni di caselle di posta elettronica**. Ad Arezzo c'è la principale web farm con 10 mila server. Un altro datacenter è a Bologna per il recupero dei dati e uno a Milano per il supporto. L'altra web farm è in Repubblica Ceca e serve l'Europa Orientale

L'incendio

È avvenuto nell'**area Ups** dove ci sono i gruppi di continuità che assicurano l'energia elettrica in caso di blackout. Aruba, per sicurezza, ha spento tutti i server, **mandando offline** per diverse ore migliaia di **siti** e caselle di **email**

* Le tecnologie e le attrezzature necessarie per pubblicare un sito web su internet