IN CYBER GUERRA ma senza un euro

Attacchi informatici ai treni, agli aerei, agli acquedotti. Ecco cosa fa (e non fa) il nostro Paese per difendersi

DI ALESSANDRO LONGO

La stazione è chiusa al pubblico: dopo un attacco informatico, i treni sono controllati dai cybercriminali. Lo stesso accade alla rete elettrica e quindi la città è piombata nel buio. Mentre i segreti industriali delle Forze Armate e del design made in Italy sono finiti nelle mani di una potenza straniera.

Scenari apocalittici, certo, ma è l'immagine di un rischio concreto. Non a caso l'Italia, anche se in ritardo sugli altri Paesi europei, sta aprendo il primo centro statale che affronterà in modo organico i problemi della sicurezza informatica. È un Cert (Computer emergency response team) istituito con il decreto della presidenza del Consiglio il 19 marzo. Una complessa struttura tecnica e operativa che affronterà il problema come una minaccia reale all'intero sistema Paese e alle nostre infrastrutture critiche (reti, banche, trasporti...).

Possiamo dire che la sicurezza informatica è diventata anche da noi un affare di Stato. Meglio tardi che mai, visto che altrove il tema riceve da tempo ben altra attenzione istituzionale. A metà marzo, la telefonata con cui Barack Obama si è congratulato con il nuovo presidente cinese Xi Jingping aveva in cima due temi: la minaccia nucleare della Corea del Nord e i continui attacchi informatici che arrivano dalla Cina, via Internet, alle aziende americane (spesso per il furto di segreti industriali). In quegli stessi giorni, le tivù e le banche della Corea del Sud sono state paralizzate da malware (software malevolo) forse proveniente dalla Corea del Nord.

«Il nostro Paese è uno dei pochissimi in Europa a non essere dotato di un Cert nazionale. Il risultato è che, quotidianamente, io e molti altri colleghi riceviamo segnalazioni, dall'estero o nazionali, su attacchi, intrusioni, frodi e attività sospette, ma manca un punto centrale al quale inoltrare queste segnalazioni, che agisca da accentratore e facilitatore», spiega Raoul Chiesa, uno dei primi hacker e oggi esperto del tema con incarichi presso l'agenzia delle Nazioni Unite Unicri e l'Enisa (European Network & information Security Agency).

«Questo decreto fa ben sperare, finalmente anche da noi si è presa coscienza del problema, della sua gravità e dei tremendi impatti, sociali, economici, politici e militari, che un attacco cyber potrebbe avere sull'Italia», continua Chiesa.

«Ci sono rischi gravissimi», concorda Umberto Rapetto, ex generale della Guardia di Finanza esperto in sicurezza informatica. «Uno dei più concreti: i cybercriminali attaccano i server Dns che tutti noi usiamo per navigare. La conseguenza è che ci ritroviamo su un sito fasullo, che in apparenza è del tutto identico, per esempio, a quello dell'Inps o della nostra banca ma è in realtà controllato da criminali. E qui ci possono rubare i nostri dati o soldi», continua. «Ma negli Usa è già successo anche che cybercriminali cinesi sono riusciti a controllare i sistemi informatici di reti elettriche e fognarie», aggiunge Rapetto.

AGOSTINO RAGOSA, NUOVO DIRETTORE DELL'AGENZIA DIGITALE CREATA DAL GOVERNO

Altro pericolo: «Nel nostro Paese la quasi totalità della aziende sono piccole e medie imprese. Sono loro il target più interessante per economie ostili che cercano la via rapida ed economica allo sviluppo, attraverso l'accesso a proprietà intellettuale sviluppata da altri», spiega Andrea Rigoni, direttore generale del Global cyber security center (fondazione di Poste Italiane) e consulente del governo per questi temi.

«Il problema è che per esigenze di business tutte le organizzazioni si sono aperte per consentire l'accesso alle proprie reti ovunque e a chiunque. Questo facilita lo sviluppo economico ma rende la gestione della sicurezza molto più complessa», dice Massimo Vulpiani, country Manager di Rsa Italia, una delle principali aziende specializzate in consulenza sul cyber crime.

«Un attacco di tipo Ddos (Distributed denial of service) può mandare in tilt un'infrastruttura di controllo della rete energetica, "sparando" una grande quantità di dati da molti computer contro un server», aggiunge. «Chi produce armamenti, invece, teme sempre il furto dei segreti industriali da parte di altri Stati. Un Paese si ritrova così i suoi aerei, costati milioni di euro in progettazione, riprodotti tali e quali in un ▸

Foto: A. Herzau - Laif / Contrasto, R. Squillantini - Imageeconomica

ercito nemico o comunque diverso. È già ccesso, secondo me anche in Italia».
Ne parla anche la recente relazione al rlamento del Sistema di informazione r la sicurezza della Repubblica (presso presidenza del Consiglio). I pericoli ncipali vengono - a quanto si legge lla relazione - dalle organizzazioni cri-inali (come anche la nostra mafia), da ati nemici, da terroristi e a volte anche da tivisti politici (come Anonymous). Gli biettivi cambiano a seconda dell'attac-nte: rubare soldi, proprietà intellettuale, greti di Stato, mandare in tilt reti o siti. nonymous, ad esempio, lo scorso febbra-ha alterato i siti del tribunale di Milano lel Dipartimento di polizia penitenziaria r pubblicare un messaggio contro «quei linquenti che ci governano».
Ora l'Italia si è decisa ad affrontare questi oblemi tutti insieme, con una struttura ntrale. Prima venivano gestiti da diversi ti e aziende private separatamente, tra cui Telecom Italia con i suoi due centri di Roma e Milano. Ma non mancano dubbi sull'efficacia del nuovo Cert. Primo problema è che il nuovo organismo deve nascere «senza oneri a carico dello Stato», come stabilisce il decreto. Laddove gli Usa e il Regno Unito hanno destinato centinaia di milioni a questo scopo. Secondo problema: non c'è chiarezza sull'organigramma del Cert e la governance è troppo articolata, a quanto fa notare Rigoni. Il Cert sorgerà come struttura del ministero dello Sviluppo economico, ma avrà numerose teste a cui dare retta. In cima alla piramide il decreto designa il presidente del Consiglio e i sei ministri del Cisr (Comitato interministeriale per la sicurezza della Repubblica); stabilisce poi un organismo collegiale di coordinamento e un Nucleo per la sicurezza cibernetica istituito all'interno dell'Ufficio del Consigliere militare. Un ruolo avrà anche la neonata Agenzia per l'Italia Digitale diretta da Agostino Ragosa: costruirà centri per la sicurezza informatica delle pubbliche amministrazioni. «Il decreto è poco chiaro sui ruoli nel Cert nazionale», dice Rigoni.

Il governo Monti ha creato una task force, ma "senza oneri per lo Stato": in nessun altro Paese è così

«Ma il problema principale è un altro: il decreto stabilisce che gli operatori telefonici devono concedere l'accesso degli organismi di sicurezza nazionale alle loro banche dati», dice Fulvio Sarzana, giurista esperto di diritto delle nuove tecnologie. «Quindi il governo, e soprattutto i servizi di sicurezza, potranno avere i dati personali dei navigatori senza dover più passare da un procedimento giudiziario», teme Sarzana. La sicurezza, nell'era del digitale, è a rischio su numerosi nuovi fronti. Compreso il pericolo di norme che, in nome di questa stessa sicurezza, indeboliscono i diritti civili. ■

Troppi computer infetti

COLLOQUIO CON FRANCO BERNABÈ

È importante la nascita del primo centro azionale per la sicurezza informatica. l governo italiano si è finalmente accorto he il problema è serio e lo sarà sempre iù man mano che tutte le persone, oggetti e nfrastrutture critiche vanno su Internet». ranco Bernabè, presidente di Telecom Italia, pplaude al decreto con cui l'Italia ha istituito n Cert (Computer Emergency Response eam). «Però altrove, e soprattutto negli Stati Jniti, la sicurezza informatica è gestita come na nuova forza armata a tutti gli effetti, on le adeguate risorse economiche. Da noi il decreto dice che questo deve vvenire "senza oneri a carico dello Stato": i mette in condizione di debolezza...»

Che cosa rischia l'Italia?

Teniamo conto che la sicurezza del Paese lipenderà sempre più dal grado di sicurezza he si riesce a dare a Internet. Gli Usa hanno già capito: hanno stabilito che inviolabilità del territorio include ra anche le reti informatiche, oltre ai tre ronti tradizionali (confini terrestri, marittimi aerei). I due virus più devastanti negli ultimi empi sono nati per compromettere e centrali nucleari iraniane; indicano che la apacità di aggredire sistemi critici da parte li malware è estremamente elevata. Noi orriamo rischi anche maggiori perché siamo ra i Paesi che hanno più problemi dal punto di vista della sicurezza informatica. Siamo al quarto posto nel mondo per presenza di computer infettati da virus. E Roma è la seconda città al mondo con questo primato».

Teme qualcosa di particolare?

«Se abbiamo così tanti computer infetti, vuol dire che alcuni dei nostri sistemi critici possono essere compromessi con grande facilità. I rischi riguardano le grandi istituzioni finanziarie, le singole imprese che devono proteggere la riservatezza delle informazioni che gestiscono. E i singoli cittadini che rischiano di mettere a disposizione di criminali i propri dati personali ed economici».

Perché Telecom si interessa di questo problema?

«La maggior parte del traffico dati italiano viaggia sulla nostra rete. Abbiamo la responsabilità nei confronti dei nostri clienti e del Paese di garantire che tutto funzioni, per quanto è nelle nostre facoltà».

Ma praticamente che cosa potete fare per la sicurezza informatica nazionale?

«Ci siamo già attrezzati con due centri Soc (Security operations centers) che a Roma e Milano fanno un'attività molto importante: rilevano il malware circolante sulle nostre reti, impediscono la paralisi funzionale dei sistemi presi di mira dagli hacker, garantiscono che i server Dns (che gestiscono l'instradamento in Rete e l'accesso ai siti Web, ndr) non vengano manomessi dai cybercriminali. Hanno un sistema di intelligence per capire da dove vengono i pericoli e quale infrastruttura può essere attaccata. Hanno la responsabilità di reagire agli attacchi informatici».

In futuro che cosa farete?

«Continueremo a potenziare il nostro sistema e pensiamo di sviluppare un'attività di protezione nei confronti di terzi. Per ora lo facciamo per i nostri clienti e laddove venga richiesto per esigenze di sicurezza nazionale siamo pronti a fornire un sistema di difesa, supporto e assistenza già collaudato e predisposto per eventuali ulteriori irrobustimenti. Ma è un'attività che pensiamo di sviluppare anche con un'offerta commerciale dedicata».

Foto: P Tre - A3