Rassegna del 13/01/2017

TRASPORTI, POSTE E TELECOMUNICAZIONI

la Repubblica

13-GEN-2017
pagina 1
foglio 1 / 4

Solo tre anni fa, in ritardo rispetto all'Europa, il governo ha varato un sistema di protezione. Poi però si è dimenticato di finanziarlo. Così siamo ancora all'anno zero

Cybersicurezza

Pochi uomini e disarmati le barriere fragili dell'Italia contro la minaccia hacker

L'INCHIESTA

La trincea desolata che difende l'Italia dai cyber-attacchi

GIANLUCA DI FEO

La centrale che vigila sugli enti pubblici ha 5 persone in tutto e funziona solo in orario d'ufficio: "Facciamo sicurezza per sentito dire". Mentre le gelosie tra militari e civili vanificano il coordinamento

Non esistono regole né strumenti per condurre attacchi contro gli incursori del web
Il generale Taricco: "Non abbiamo capacità nazionali per produrre sistemi e software blindati"

AVREMMO potuto stupirvi con effetti speciali, ma la realtà della rete di sicurezza informatica nazionale è molto povera. Ricca di idee e di buona volontà, misera di risorse e di personale. Così se scendiamo nelle trincee che dovrebbero difendere il Paese dalle orde di predatori di dati, che si tratti di guastatori russi o dei fratelli Occhionero, le troviamo desolatamente sguarnite.

LE TRE fortezze che hanno il compito di proteggere l'Italia dalle grandi incursioni digitali — per intenderci, non stiamo parlando dei truffatori che cercano di afferrare soldi dai conti ma delle offensive che possono mandare in tilt interi ministeri o violare le comunicazioni del governo — si chiamano Cert, Computer emergency response team: sono le centrali operative incaricate di scoprire gli assalti e sincronizzare la risposta. La più importante, un po' enfaticamente battezzata "Cert Italia", dovrebbe coordinare tutte le realtà pubbliche e private in un unico scudo online ma ha un organico di «una decina di persone». Il "Cert Pubblica Amministrazione" invece è la barriera degli enti statali o locali che però funziona «in orario d'ufficio, anche se pure il sabato o la domenica si trova qualcuno che risponde al telefono». Come se gli hacker riposassero la notte o si astenessero dalle razzie nel weekend. D'altronde non si può chiedere ai due funzionari e ai tre tecnici precari che lo presidiano di fare i salti mortali. Il responsabile Mario Terranova spiega che «è un Cert che gestisce la sicurezza per sentito dire, perché non ha sonde sue, non c'è il videowall su cui si accendono gli allarmi, ma le segnalazioni più importanti derivano dalle attività di monitoraggio che effettuiamo al nostro interno».

Infine c'è il Cert Difesa, il più dotato e reattivo seppur costruito con un investimento complessivo di 15-20 milioni: meno del costo del motore di un F-35, meno di un millesimo della spesa annuale per le forze armate. Complessivamente possiamo contare su una quarantina di paladini per vigilare la frontiera digitale del Paese, che ha confini virtuali ma custodisce interessi colossali perché lì scorre tutta la nostra vita: una sovranità a dir poco limitata, se non inesistente.

La fragilità della cyber-muraglia è stata esplorata dalla Commissione Difesa della Camera presieduta da Francesco Saverio Garofani, con una rara indagine conoscitiva sul tema giusto al momento ingiusto che si concluderà entro primavera. I lavori dei deputati sono partiti proprio mentre l'allora capo del governo Matteo Renzi po-


la Repubblica
Dieselgate, gli Usa contro Fca: fuorilegge più di 100 mila auto

la Repubblica

13-GEN-2017
pagina 1
foglio 2 / 4

neva la questione della sicurezza informatica, stanziando 150 milioni per creare una nuova autorità di sorveglianza con ampi poteri: un intervento sacrosanto, viziato però dalla manifesta indicazione di affidarne la guida all'amico Marco Carrai.

Che serva un'unica struttura in grado di gestire le emergenze cibernetiche lo impone l'Europa, con una direttiva da attuare entro il prossimo anno. Ed è dal 2004 che l'Ue ha lanciato l'allarme, in anticipo rispetto al primo grande cyber-attacco della storia: l'irruzione sul fronte orientale dell'Unione che nel 2007 ha quasi paralizzato l'Estonia. Noi ce la siamo presa comoda e solo nel 2013 con il governo Monti abbiamo varato un sistema di protezione, dimenticandoci però di finanziarlo: sulla carta gli organismi ci sono, fondi e uomini invece latitano. E stiamo parlando di un campo dove tutto invecchia in fretta, tanto che la nostra rete di coordinamento è considerata già superata. Oggi la speranza di attivarsi velocemente in caso di brecce telematiche è utopica, ostacolata da un organigramma troppo articolato e poco funzionale. Persino le esercitazioni sono una rarità: il "Cert Pubblica amministrazione" ne prevede una ogni anno, il "Cert Italia" addirittura con cadenza biennale. Le audizioni della Camera mettono in risalto l'impegno collettivo per trovare rimedi mostrando però un settore dominato dall'intreccio di gelosie e culture diverse: civili e militari, aziende private ed enti pubblici, restii a condividere debolezze e virtù. Nessuno ama sbandierare la falla nei server e i danni subiti: i cyber panni sporchi si lavano in famiglia. Così non si riesce a fare tesoro degli errori e mettere sull'avviso le prossime vittime.

Siamo all'anno zero: i server di Asl e Regioni non sono nemmeno al riparo dai ladri vecchia maniera, figuriamoci dagli hacker. Il direttore di Italia Digitale Antonio Samaritani ha spiegato che su 896 data center analizzati, il 40 per cento non ha neppure il "certificato di agibilità fisica" mentre un terzo non ha le dimensioni minime per inserire schermature contro i predoni cyber. I custodi ministeriali criticano la scarsa collaborazione dei militari: «Non partecipano alle nostre esercitazioni, non scambiano dati — dichiara il dottor Terranova — , anche se i fatti seri che sono successi hanno dimostrato che i computer non hanno divisa, per cui se il computer della Difesa viene compromesso, compromette anche quelli degli altri. Per questo è necessario il dialogo e la cooperazione». Il generale Giandomenico Taricco, capo dell'intelligence militare, invece punta l'indice sulle macchine che arrivano già "fallate" negli uffici civili: «La loro regola fondamentale è comprare al massimo ribasso. Spesso significa comprare il computer cinese: è probabile che coloro che sono dietro al computer cinese siano scaltri e riescano a venderci lo strumento col quale poi ci ruberanno le informazioni».

Lo Stato maggiore della Difesa ha la struttura più professionale e una visione strategica chiara. I militari gestiscono una sala operativa sempre aperta e stanno per inaugurare un super-comando per le cyber-operazioni. Si sono resi conto che questo sarà il campo di battaglia fondamentale non del futuro ma del presente. Lo hanno fatto a loro spese, visto che sono stati vittima di almeno un raid — rivelato da Repubblica — con una sospetta matrice russa. Anche i generali però sono a corto di soldi, con acrobazie illustrate dall'ammiraglio Ruggiero Di Biase persino per pagare il rinnovo delle licenze dei software. E se lo scorso anno hanno beneficiato di una decina di milioni, parte dei fondi renziani, nel bilancio 2017 non si prevede un solo euro. Questo mentre la Germania ha stanziato un miliardo per armare una panzerdivision cibernetica forte di 13.500 soldati che proteggerà enti pubblici e società private.

I nostri militari non si perdono d'animo e sono pronti ad allestire una linea del Piave per sorreggere il resto delle istituzioni. Con meno di tre milioni, hanno creato una sorta di "autostrada digitale" fortificata in cui convogliare i dati più riservati mettendola a disposizione degli altri ministeri. E qui nasce un altro dilemma, assolutamente inedito. Perché per scoprire gli attaccanti prima che provochino danni colossali, è necessario infiltrare delle sentinelle nei server: osservatori invisibili per avvistare i nemici mentre scavano le brecce. Già, ma con quali garanzie si può permettere ai commandos del web di gironzolare tra i file delicati — ad esempio — della Giustizia o di Palazzo Chigi?

Ci vogliono regole di ingaggio e organismi con poteri di controllo, indispensabili pure per sciogliere un altro nodo chiave: come autorizzare e condurre i nostri assalti cibernetici? Gli esperti sono concordi nel sostenere che in questo settore la difesa può essere solo attiva: come in un duello di scherma, non basta parare un colpo ma bisogna immediatamente replicare con una stoccata, altrimenti ti arriverà un altro fendente. Serve una rappresaglia mirata, quantomeno per neutralizzare la sorgente dell'affondo. Davanti ai deputati, l'ammiraglio Di Biase ha dichiarato che l'Italia oggi non è in grado di condurre azioni offensive. Manchiamo quindi di deterrente: chi ci assale, sa che non ci saranno ritorsioni. Mentre l'onorevole Massimo Artini ha sottolineato come l'Olanda solo annunciando la "licenza di uccidere" per i suoi cyber-custodi abbia dimezzato gli attacchi subiti.

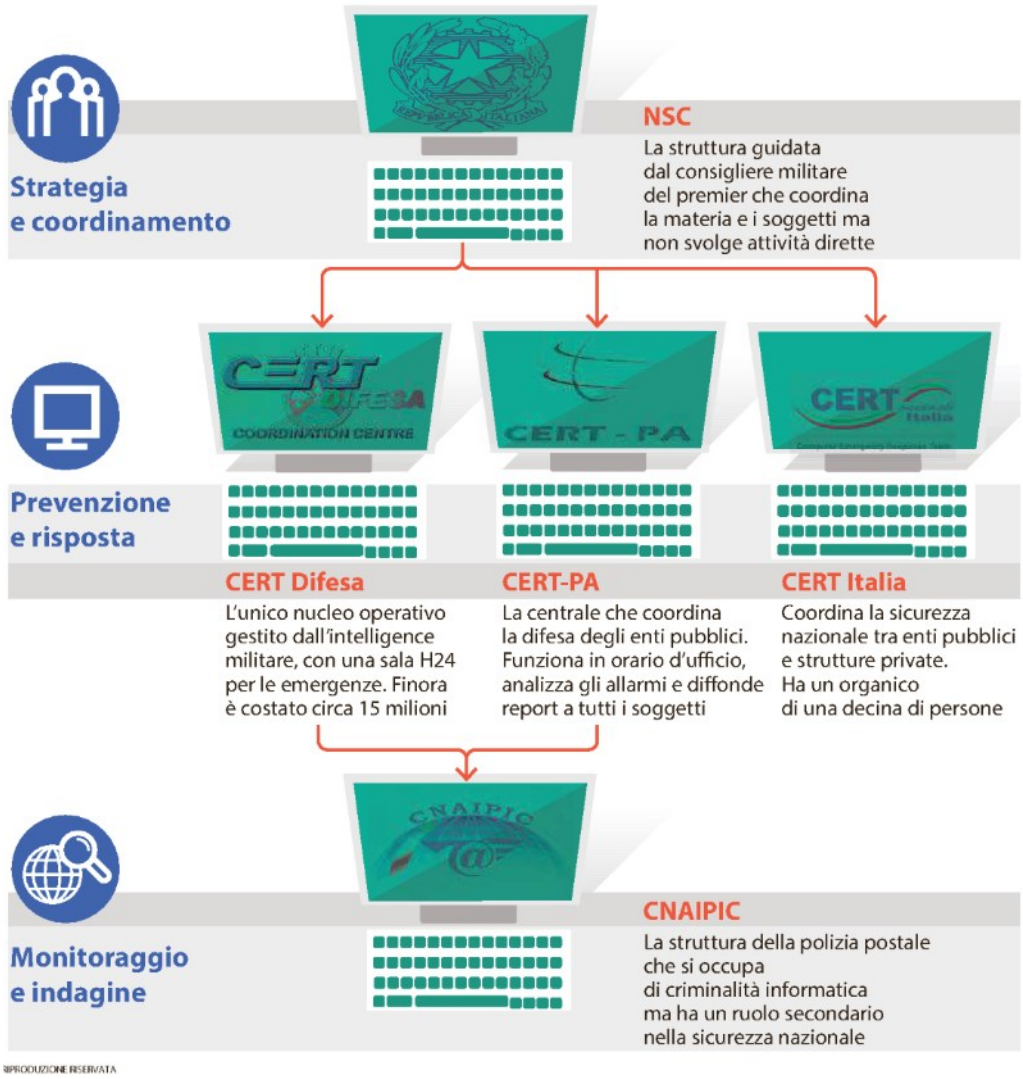
E i nostri 007 come si muovono? Ovviamente è top secret. Il Dis — l'organismo al vertice dell'intelligence — viene accreditato come la maggiore cyber-potenza italiana. E in attesa delle future riforme, più di cento dei milioni stanziati da Renzi sono stati parcheggiati nelle casse dei servizi segreti. Un tesoretto che ancora non si sa chi spenderà e come. Il mercato dei sistemi di sicurezza cibernetica è dominato dalle aziende israeliane, ma tutti i paesi hanno bisogno di macchinari di provata fedeltà. Perché in questo mondo — ha evidenziato il generale Taricco — «non esistono alleati. La battaglia è principalmente economica e, quindi, siamo tutti alleati, ma siamo anche tutti competitivi, perché ognuno comunque vive di competizione». Al momento, «non abbiamo capacità nazionali né dal punto di vista hardware, né dal punto di vista software. Ciò significa subire gli altri, con tutto quello che comporta. Infatti, quando si compra un server, si rischia di acquistare anche la porta attraverso la quale chi vuole può estrarre le informazioni». In

la Repubblica

13-GEN-2017
pagina 1
foglio 3 / 4

Italia esiste qualche picco di eccellenza. Selex — il ramo elettronico di Leonardo-Finmeccanica — ha vinto l'appalto per la Nato e gestisce un'agguerrita sala operativa a Chieti. Elettronica, Vitrociset e una pattuglia di start up hanno cominciato a sfornare brevetti. C'è poi un consorzio di università dinamico nella ricerca. Tutti però senza finanziamenti e senza una regia di governo. Una falla che va turata. In ballo c'è la sovranità nazionale. E, come sintetizza il generale Taricco, «se non riusciamo ad agire in maniera efficace, saremo inconsistenti».

Sistema nazionale di sicurezza cibernetica



I PERSONAGGI

IL GENERALE
Carmine Masiello, consigliere militare del premier, è al vertice del Nsc che coordina la sicurezza cibernetica e a cui fanno riferimento tutte le strutture

IL DEPUTATO
Francesco Saverio Garofani presiede la Commissione Difesa della Camera che conduce l'indagine sulla cybersicurezza. Le audizioni sono state pubblicate online

il Giornale

13-GEN-2017
pagina 4
foglio 1

L'EX HACKER Roberto Martelloni

«Il crimine ormai buca la rete La tecnologia è l'unica difesa»

Internet è il nuovo campo di battaglia dove si gioca il futuro

Guerre
Spionaggio senza esclusione di colpi

Costi
Usare un server negli Usa costa 5 dollari

Giorgio Stamatopoulos

«La cybersicurezza è un tema complesso, e bisognerebbe investire di più non solo sulle tecnologie ma anche su chi le deve usare. La vicenda EyePyramid lo dimostra». Partito da Milano quasi 20 anni fa come giovane pirata della rete, Roberto Martelloni ha cominciato a occuparsi di sicurezza informatica quando era ancora un concetto astratto, affidato alla sperimentazione. Oggi, dopo aver lavorato per aziende come Eni e Finmeccanica, vive a Dublino e lavora per Citigroup, colosso dei servizi finanziari, dove gestisce tutta la strategia che riguarda la sicurezza dei device mobile (MID).

Partiamo dall'inchiesta della procura su Giulio Occhionero, che porta diretta agli USA, passando per una società satellite di Finmeccanica, la Westland. Cosa le suggerisce?

«Che fra le varie aziende di Finmeccanica e della difesa possano esserci lotte e cordate di potere interne non stupisce. E che questo caso tracci una linea relativa a spionaggio interno è grave, lo spionaggio lo è di per sé. Ma se un ingegnere senza particolari capacità tecniche, può intercettare comunicazioni e account di politici e finanzieri è evidente che qualcosa non va».

Quanto è costoso mettere in piedi una struttura così?

«Ormai c'è un vero mercato del cybercrime, e certi strumenti nemmeno si comprano più, si possono affittare per meno di cinquemila euro. Usare un server negli Stati Uniti costa meno di 5 dollari al mese».

Chi sono i clienti più interessati ad un tale servizio?

«Da quel che è venuto fuori, le intrusioni spaziavano dalla politica all'economia, e in alcuni casi gli ambiti erano anche sovrapponibili, quindi è difficile fare speculazioni. Ma lo spionaggio in appalto e subappalto, è una realtà ormai comune anche in Italia, perché nel «pubblico» non ci sono capacità di effettuarlo, quindi ci si appoggia spesso ad aziende private, che sono tante. A Milano per esempio, abbiamo HackingTeam, ma c'è anche Area, una tra le maggiori aziende private del settore delle intercettazioni telematiche».

Wikileaks e post verità. Davvero la rete è diventata il nemico pubblico numero uno?

«Internet è solo un altro mezzo per condividere informazioni. Quindi tutti i problemi che già affliggono il giornalismo, come la propaganda e la strumentalizzazione delle notizie, trovano nella rete un mezzo in più per aver luogo. Per quanto riguarda l'aspetto più politico della faccenda, a Tallinn in Estonia, i vertici militari americani e NATO, insieme ad avvocati ed esperti, stanno già studiando come regolamentare il futuro delle cyberwar e dello spionaggio».

Per elaborare una sorta di convenzione di Ginevra delle guerre cibernetiche?

«Esattamente. Ed esiste già un Tallinn Manual, per definirne limiti e regole».