Storia di copertina

Virus informatici

Sorpresa: il web sotto attacco è colpa nostra

» VIRGINIA DALLA SALA

Città connesse, auto connesse, frigoriferi connessi, lavastoviglie, condizionatori, semafori, dighe, sistemi elettrici, tv, computer, antifurti, vestiti, orologi, strumenti salvavita: il futuro, come lo vede il mondo e come lo vede l'Europa, si chiama *Internet of Things*, internet delle cose. Tradotto: tutto collegato con tutto e tutto connesso a Internet. Con un enorme rischio: le conseguenze degli attacchi informatici potrebbero essere molto più vaste di quanto la crisi informatica della scorsa settimana ha mostrato. I Paesi, le istituzioni, gli stessi cittadini non sono ancora pronti ad affrontarne una nuova. E soprattutto, ad evitarla

ROMA-BRUXELLES. Marzo 2017: Commissione Europea, Consiglio e Parlamento firmano una dichiarazione d'intenti congiunta per accelerare il raggiungimento degli obiettivi per il Mercato unico digitale. Tra i progetti, la connessione di tutto il sistema dell'automotive europeo. È il motivo per cui premono sul potenziamento della connessione di rete (fibra ottica e 5g): sono convinti che creare una condizione di costante connessione contribuirà a garantire sicurezza e servizi, a monitorare lo stato delle infrastrutture, contenere le spese, prevenire gli incidenti e finanche contrastare il terrorismo. In questo sogno europeo, c'è però un problema non secondario: la cybersecurity. "È una questione urgente - spiega Roberto Viola, l'italiano a capo della Direzione Generale per Comunicazione Digitale e Tecnologie della Commissione Europea - la settimana scorsa, a Terna, ho partecipato a un workshop sulla sicurezza delle reti energetiche: gli operatori sono consapevoli che la loro sicurezza dipende da quella informatica. Lo stesso vale per i trasporti e per le transazioni finanziarie".

SICUREZZA. Viola spiega che oggi le minacce arrivano da più parti: dai cybercriminali, come per il virus Wannacry che con un ricatto informatico provano a estorcere soldi, e dai paesi ostili, che usano gli attacchi informatici come arma di offesa. "Sono entrambe questioni enormi, sulle quali l'Europa non può farsi trovare impreparata". Eppure, tra i vari Paesi non c'è coordinamento, tanto che la direttiva sulla cybersicurezza che sarà discussa nei prossimi mesi imporrà agli stati dell'Unione di cooperare e ai vari sistemi di difesa di condividere le informazioni. Anche perché la strategia in vigore ora risale al 2013: "Non viene neanche citata l'Iot - dice Viola -. Per questo dobbiamo assolutamente aggiornarla a settembre, prevedendo ad esempio che tutti gli oggetti connessi abbiano anche una certificazione unificata sulla sicurezza. Questi criminali organizzati non si battono facilmente. Certo, c'è la sicurezza di cui si fa carico l'intelligence nazionale, ma da sola non basta". E ora, anche in Europa, stanno cercando di recuperare il tempo perduto.

RAPINE. A fornire un quadro della gravità della situazione è Evgenij Kaspersky, miliardario, guru della virologia informatica e fondatore di una delle più grandi aziende produttrici di antivirus al mondo, nella prefazione del romanzo *Il nodo di seta* (Sandro Teti Editore). "Nel 2014 - scrive - abbiamo aiutato diverse banche dell'Europa dell'Est ad affrontare attacchi informatici. Abbiamo scoperto una banda di hacker (soprannominata da noi "Carbanak") che aveva messo in atto nel tempo, con tutta probabilità la più grande rapina bancaria della storia: crediamo che sia stato rubato quasi un miliardo di dollari da un gran numero di istituti bancari nel mondo". Durante le indagini si accorgono che il primo malware, il software malevolo usato per il furto, era stato elaborato un anno prima. "Ho ripetuto più volte - dice Kaspersky - che i criminali si sarebbero concentrati maggiormente sulle banche. Quello che non avevo previsto era che si sarebbero concentrati anche sulle Banche Centrali".

OBIETTIVI SENSIBILI. Si riferisce all'attacco alla Banca centrale del Bangladesh, nel 2016. I pirati informatici riuscirono a prendere il controllo del sistema di trasferimento fondi ed emisero 35 richieste di transazioni finanziarie per un valore totale di 951 milioni di dollari. "Trenta transazioni furono bloccate dalla Federal Bank di New York e, a quanto pare la ragione dello stop fu un errore nella descrizione del destinatario (avevano scritto Fandation invece di Foundation). Nonostante ciò furono rubati più di 80 milioni".

NEL PICCOLO. Dalla larga alla piccola scala, la cyber security è un sistema a catena. I virus si trasmettono, i malware si installano e si nascondono, i worm strisciano e si moltiplicano. L'origine è sempre umana: la mano di chi apre un allegato di una mail infetta o l'errore di chi commette errori nelle stringhe di codice che costituiscono l'architettura dei sistemi informatici. E ogni vulnerabilità è la porta di accesso per i criminali informatici. Che restano quasi sempre impuniti. "I crimini informatici - spiega Kaspersky - non sono semplici da scoprire e molto spesso ancor più difficili da perseguire. Molti sono contrastati efficacemente, ma raramente gli hackers finiscono in prigione. Molto spesso continuano a ingegnarsi per colpire con nuove modalità".

COLPA NOSTRA. Le vulnerabilità, quindi, ci sono e ci saranno sempre. Nella struttura di siti e programmi ma soprattutto nel comportamento degli utenti. C'è quello che apre l'allegato infetto ma ci sono anche tutti coloro che non tengono conto dell'importanza di avere in azienda o nella Pubblica Amministrazione una efficiente struttura incaricata della manutenzione dell'apparato informatico. L'attacco Wanna Cry che ha bloccato ospedali e anche un'azienda di telefonia ha interessato soprattutto le postazioni dotate di sistemi operativi ormai obsoleti come WindowsXP o Windows Server 2003: nes-

Il libro

• **Il nodo di seta**
Marco Forneris
Pagine: 232
Prezzo: 16 €
Editore: Sandro Teti Editore

La scheda
WANNACRY
Detto anche WCry, WanaCrypt, Wanna Decryptor e WanaCrypt0r, significa "voglio piangere"
È un ransomware, un malware estremamente pericoloso che si insedia nel sistema operativo e cripta tutti i file salvati sull'hard disk e su eventuali chiavette Usb collegate
Poi, chiede al proprietario del device di pagare in riscatto in Bitcoin (valuta elettronica non rintracciabile) se vuole riavere i suoi documenti
Ha colpito i sistemi operativi non aggiornati, come Windows XP

Valuta virtuale In pagina, la sede Ue a Bruxelles e la "guida" di WannaCry che spiega come pagare il riscatto in bitcoin *Ansa/La-Presse*

DOPO LA CRISI DI WANNACRY L'EUROPA SI SCOPRE IMPREPARATA, GLI UTENTI TROPPO INGENUI, LA PA NON CONTROLLATA. E CON L'INTERNET DELLE COSE, TUTTO SARÀ CONNESSO

Cibersecurity *Ogni giorno vengono inventati fino a 20mila virus. Non facciamone un incubo, ma non sentiamoci mai al sicuro. Pure le informazioni delle persone comuni fanno gola*

L'INTERVISTA

Umberto Rapetto

"Anche un uomo solo può mandare in tilt un intero Paese"

» FERRUCCIO SANSA

State attenti alle app! Nessuno è al sicuro: si va dai sistemi informatici dei governi al computer e ai telefonini di casa. Passando per multinazionali, banche, borse, giornali e ospedali.

Umberto Rapetto, lei ha fondato il Gat (Gruppo anticrimine tecnologico) della Guardia di Finanza. Ha condotto la famosa indagine sull'evasione delle slot. Era soprannominato lo "sceriffo del web". Cos'è la cybersecurity e come difenderci?

Distinguiamo: si parla di sicurezza cibernetica quando ci riferiamo a sistemi per prendere decisioni strategiche. Deriva dal greco *kyber*, timone, che ritroviamo nel latino *guber*... governo.

Cybersecurity, sembra una parola remota. Come può toccare la nostra vita?

Non sono solo governi e istituzioni a subire attacchi informatici, ma anche chi eroga servizi essenziali come energia, trasporti, sanità, telecomunicazioni e finanza.

Partiamo dai governi.

È una guerra incessante.

Come ai tempi della guerra fredda?

Adesso siamo in un mondo tripolare: Stati Uniti, Russia e Cina. Sembrerebbe scongiurare il tanto temuto scontro definitivo perché nessuno può combattere contro due nemici nello stesso tempo.

Ma gli attacchi arrivano soltanto dagli stati nemici?

Nelle guerre convenzionali combattevano solo i grandi eserciti. Oggi anche una sola persona può mettere in ginocchio un'intera Nazione: i pirati digitali non sono più le figure mitiche e romantiche di un tempo, ma hanno una connotazione venale e sono pronti a lavorare per criminalità e servizi segreti.

E poi ci sono multinazionali e imprese...

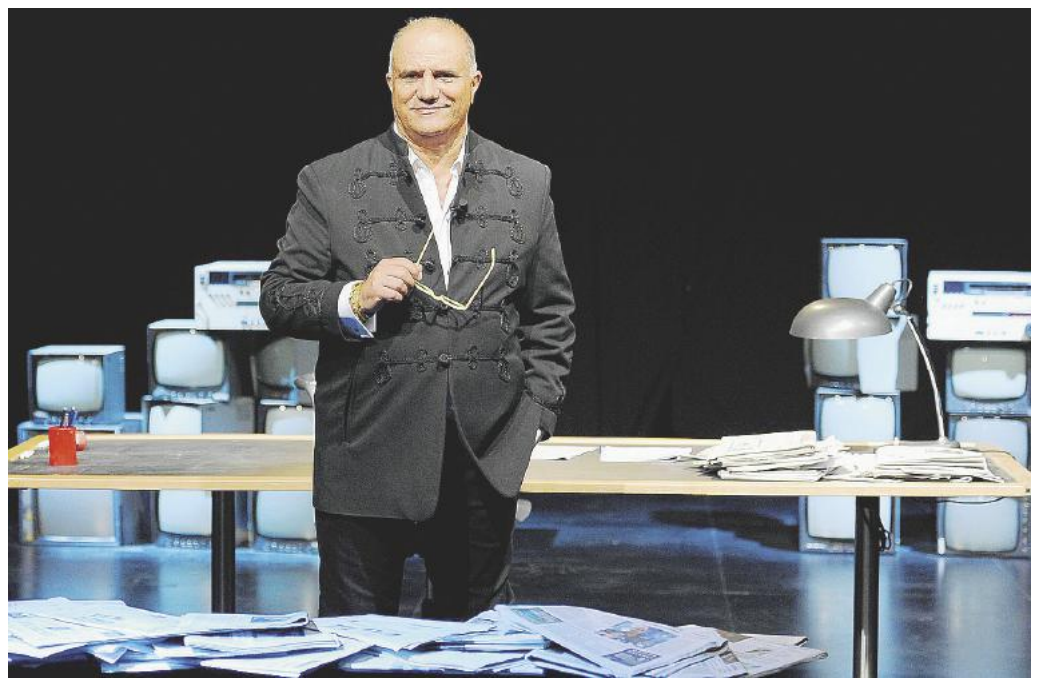
Le multinazionali affrontano i concorrenti rubando le informazioni e ostacolando il lavoro. Intrufolarsi nella posta elettronica di una azienda, alterare il contenuto della contabilità o degli archivi, paralizzare i processi produttivi sono mosse ricorrenti.

È fantascienza o vita reale?

Il blocco delle attività degli ospedali appena avvenuto in Inghilterra dimostra la concretezza del pericolo. In Italia *Wannacry* non ha fatto quei danni per l'arretratezza dell'informatizzazione ospedaliera, ma altri "virus" avevano già creato enormi disagi in Asl e strutture cliniche. L'Italia è già stata bersaglio.

Chi è

Ex colonnello della GdF, Umberto Rapetto ha fondato e diretto il Gruppo anticrimine Tecnologico È tra le massime autorità in tema di cybercrime Nel 2012 scoprì una colossale evasione fiscale - si parlava di 98 miliardi di euro - da parte dei "signori delle slot" Dimessosi non senza polemiche dal suo incarico, si è dato all'insegnamento e alla tv. È il ceo di di Hkao



Come si attacca una banca?

La finanza è facile preda: un rallentamento dei sistemi che gestiscono le operazioni di borsa può essere disastroso. Lo spostamento della virgola può far contabilizzare per 25.000 euro un prelievo bancomat da 250.

Che cosa dovrebbero fare le imprese per difendersi?

Dare priorità agli investimenti nella formazione, ancor prima di spendere in apparecchiature e in software che invecchiano in un battito di ciglia. Le verifiche dell'eventuale vulnerabilità deve essere effettuata seriamente, i *penetration test* non devono essere "combinati" pur di ottenere certificazioni o coperture assicurative. Le soluzioni *cloud* dovrebbero essere collaudate e poi, a guardare gli utenti, si potrebbe evitare l'uso promiscuo di dispositivi aziendali (smartphone e tablet) che vengono utilizzati per i giochi o dati ai figli.

> *In Italia un attacco è meno realizzabile perché siamo più indietro: i reparti non solo collegati ancora fra di loro*

Lo Stato sta affrontando i nemici cibernetici?

Ce n'eravamo occupati prima degli altri. Nel 1995 al Sisde insegnavo nei corsi di *technointelligence*. Poi abbiamo perso tanto tempo, sprecando le migliori risorse umane d'Europa, accantonando o mettendo in fuga gli specialisti...

La guerra informatica può arrivare anche alla nostra politica?

Si può danneggiare un candidato o un partito cancellando o sostituendo contenuti nei siti, creando *fake news* o fotomontaggi, rubando identità e muovendosi sui social con comportamenti estranei ai politici da colpire.

I rischi per la gente comune quali sono?

Le app del cellulare sono il nostro tallone d'Achille. Le riteniamo gratuite ma rubano la nostra privacy, accedendo alla rubrica, ai messaggi, alla posta elettronica, alle foto: entrano nella nostra vita, costruiscono collegamenti e relazioni, ci catalogano conoscendo gusti e opinioni, preparando un nostro futuro dossier...

Come difenderci?

Installiamo solo le app effettivamente necessarie, riducendone l'invasività. Teniamo aggiornato il sistema operativo dei nostri dispositivi elettronici e i programmi antivirus. Salviamo periodicamente i file eseguendo il back-up di dischi e supporti di memorizzazione. Cambiamo sovente le password ed evitiamo di effettuare navigazioni online "pericolose" e di scaricare software non garantiti.

Non facciamone un incubo, ma non sentiamoci mai al sicuro.

I numeri

20mila
È il numero dei pc che ogni giorno vengono infettati nel mondo

150
Sono i Paesi in cui tra il 12 e 13 maggio si è diffuso l'attacco informatico WannaCry

600
Dollari in bitcoin: è il riscatto medio richiesto dai cybercriminali che ha generato 100mila dollari di utile

suno li aveva aggiornati con l'ultima versione che, di fatto, conteneva le barriere necessarie a contrastare l'attacco.

IL FUTURO. "Si è trattato di un test su scala globale - spiega Michele Colajanni, fondatore della Cyber Academy di Modena - ha coinvolto Asia, Europa. Non ha colpito l'America solo per il fuso orario. Ma c'è della colpa anche in chi è stato attaccato: sistemi operativi non aggiornati, persone che hanno cliccato. Questo ci insegna che a livello globale tutti gli uomini continuano a essere curiosi, incompetenti, e l'attaccante ha vita facilissima". É una reazione a catena: l'utente che libera il malware crea danno perché l'azienda non ha aggiornato i sistemi operativi e non ha nessun obbligo di legge a farlo. Per accorgersi di un attacco, poi, in media ci vogliono 200 giorni. "É stato uno studio sociale interessantissimo e mondiale su come stiamo messi dopo tantissimi anni di evoluzione e non all'alba della sicurezza informatica - dice Colajanni -. Siamo messi male: ed è preoccupante. Anche perché presto passeremo a una fase dove non collegheremo più solo i computer, ma le cose. I semafori, le industrie, i robot. Non ci si potrà permettere superficialità quando avremo in casa oggetti facilmente violabili. Questa crisi, paradossalmente, è valsa più di cento conferenze sulla cybersecurity".