Vicenza, 28/05/2017

WANNACRY – Una Cyber Arma popolare ed innovativa

Le cronache ci stanno sempre più frequentemente inondando di notizie riguardanti i cosiddetti cyber-attacchi. Hackers che vanno all'assalto di siti istituzionali, oltre che di anonimi computer domestici. Siti istituzionali di varia natura e dai contenuti sicuramente sempre più delicati.

Di recente ha avuto gran clamore un caso decisamente anomalo, anche se non rarissimo: il furto di cyber-armi dai sistemi di un ente che si occupa di sicurezza nazionale. Parliamo dell'assalto portato da un gruppo di hackers ai sistemi della NSA (National Security Agency), agenzia americana che ormai non ha certo bisogno di presentazioni. Uno dei sistemi (così ci si aspetterebbe che fosse e così dovrebbe essere) tra i più protetti al mondo!

Il gruppo di hackers autore dell'assalto ("The Shadow Brokers") non è nuovo ad imprese del genere ma fa sicuramente scalpore l'attuale loro blasonatissima vittima.

Non solo: ancora più scalpore desta la notizia che oggetto del furto non sono state le classiche preziose informazioni segrete ma degli oggetti informatici che si possono tranquillamente definire "cyber-armi". Armi detenute dalla NSA, provenienti da dove non è chiaro e conservate dall'agenzia per motivi tutti da scoprire, anche se ovviamente un osservatore smaliziato ha ben chiari quelli che possono essere gli obbiettivi di questo scabroso "magazzino".

Il furto, avvenuto il 14 aprile, ha comportato il fatto che una serie di tecnologie di attacco detenute dalla NSA sia finita in mani diverse e sicuramente "sbagliate". Dopo un breve periodo di studio delle "armi" rubate, sembra che i ladri abbiano approfittato su larga scala delle potenzialita' offensive degli armamenti conservati dalla NSA, con un attacco informatico di dimensioni rilevanti che ha colpito una quantità consistente di computer utilizzati in aziende ed enti di varie nazioni.

Ben (purtroppo) studiata la denominazione di questo attacco. "WannaCry" (traducibile con un "vorrei piangere") in realta' e' l'abbreviazione di "WannaCript" ("vorrei criptare") ed il gioco psicologico di questo nomignolo e' decisamente efficace.

WannaCry, da un punto di vista tecnico, rappresenta un caso atipico negli assalti informatici, in quanto e' costituito da due componenti che solitamente si presentano separati e distinti: un ransomware (programma che cripta i dati e chiede un riscatto) ed un "virus" vero e proprio che veicola il ransomware in giro per il mondo. Questo mix (decisamente esplosivo) ha avuto vita facile nei computer in cui i sistemi operativi non erano stati **perfettamente** e **tempestivamente** aggiornati mentre sembra non aver avuto possibilita' di azione sui computer i cui sistemi erano aggiornati. Ovviamente queste sono le informazioni che la comunità mondiale ha fornito sull'episodio.

Tecnicamente l'assenza di un aggiornamento di windows (la MS17-010) e la contemporanea presenza del protocollo SMBv1 costituiscono il mix esplosivo di condizioni che permettono l'attacco ad uno specifico computer. Condizione presente purtroppo in milioni di computer sparsi in giro per il mondo e presenti in aziende di ogni tipo, col risultato che la cyber-arma ha potuto assaltare un gran numero di computer.

Siamo (è bene ribadirlo) in una società profondamente governata dall'informatica. Un intricato reticolo di computer e di reti controlla gran parte del nostro habitat sociale, per cui se è vero che una guerra convenzionale può creare grandissimi danni, è altrettanto vero che un assalto informatico può creare altrettanti se non maggiori problemi. Ecco quindi che, accanto agli eserciti tradizionali, le grandi potenze hanno mosso con decisione i loro passi sul fronte delle armi cibernetiche, altrettanto distruttive e molto più facilmente maneggiabili. L'esercito tradizionale, col suo pesante apparato logistico e con i suoi movimenti difficilmente dissimulabili, sta diventando decisamente obsoleto, lento, inadeguato. Crea danni materiali perfino antieconomici. Un hacker invece, essendo privo di fisicità, colpisce ovunque sia necessario colpire senza ostacoli geografici e in modo estremamente mirato. Produce dei danni istantanei che nessun esercito al mondo riuscirebbe a

causare e, dulcis in fundo, si tratta di danni per lo più “funzionali”.

Si pone quindi il problema dei drammatici effetti sulla vita delle persone che un attacco all’apparenza cosi’ “fisicamente incruento” potrebbe avere. Il non funzionamento dei trasporti, dell’erogazione della corrente, dell’acqua, delle telecomunicazioni, dei servizi bancari e dell’informazione (per fare alcuni banali esempi) che effetti potrebbe produrre nell’odierna società? Più o meno gravi degli effetti di una guerra convenzionale? La domanda e’ malposta.

Si tratta di attacchi che hanno un effetto psicologico enorme, innanzitutto. Ma hanno anche un carattere “economico” che li rende ulteriormente appetibili: non si distrugge granché, infatti, per cui al vincitore non si pone nemmeno il problema di un territorio nemico conquistato che, ridotto ad un cumulo di macerie, va ricostruito con tutti gli oneri relativi: il low price, quindi, entra anche nell’ambito delle guerre. Che paiono essere sempre piu’ indirizzate verso il “non convenzionale”, verso il “non fisicamente distruttive” e quindi orientate in una direzione non perfettamente immaginabile, oggi.

L’esempio di cosa è accaduto ad alcuni ospedali inglesi vittima del WannaCry e’ evidente: sistemi sanitari paralizzati e, addirittura, sistemi di soccorso incapaci di intervenire. Di fatto un impatto diretto sulla salute ma anche sulla vita stessa delle persone. Fortunatamente poche, nel caso specifico. Però un assaggio in piccolo ed in breve di ciò che potrebbe accadere. Anche tenuto conto del fatto che il tipo di assalto attuale non poteva produrre effetti di durata rilevante e non ha nemmeno colpito un numero rilevante di sistemi.

Ecco quindi che nasce (ed e’ nata da un pezzo) la nuova frontiera delle guerre moderne: le guerre cibernetiche.

Naturalmente non e’ tutto qui. Ovvio che il sotterraneo mondo degli assalti informatici dà spazio non solo alle guerre canoniche e dichiaratamente tali ma permette anche un assalto generale ed articolato alle informazioni ed ai servizi informatici, con obbiettivi spesso legati all’economia, alla finanza, alle strategie geo-politiche, a tutto ciò che “fa girare il mondo”. Un insieme di contesti a cui ormai stanno da tempo guardando con estrema attenzione tutti i servizi di intelligence e le agenzie di sicurezza nazionale, oltre ai vari enti sovranazionali che in un qualche modo si occupano di sicurezza o di regolamentazione di varie attivita’ economiche o produttive mondiali.

Uno scenario in cui la Protezione Civile, nel contesto della normativa europea e nazionale più recente, che detta le linee di condotta da adottare per il rafforzamento delle reti e dei sistemi informatici, non può essere assente e non può nemmeno evitare di disegnare alcuni scenari possibili in cui un giorno (speriamo mai) potrebbe trovarsi ad intervenire per assistere la popolazione e per ricostruire il più rapidamente possibile l’infrastruttura danneggiata dal cyberattacco di turno.

Carloalberto Sartor
Security Manager

(Pubblicato su LaProtezioneCivile, Luglio 2017)