Il Sole 24 ORE

Data: 17.03.2022
Size: 413 cm2
Tiratura: 91744
Diffusione: 138603
Lettori: 713000

10 miliardi

DOLLARI
Tanto si stima sia stato il costo dei riverberi a livello mondiale del cyberattacco sferrato nel 2017 ad aziende e infrastrutture critiche ucraine mediante i *malware* NotPetya e Bad Rabbit. Tra il 2015 e il 2016 un altro *malware* chiamato BlackEnergy lasciò senza energia elettrica e riscaldamento centinaia di migliaia di ucraini.

Perché l'Europa ha bisogno di una strategia comune per la difesa informatica

Le nuove frontiere della sicurezza

Michele Colajanni, Giusella Finocchiaro e Oreste Pollicino

La guerra in Ucraina ha generato per la prima volta la paura concreta di una *cyberwar*. La minaccia cibernetica è senza precedenti in termini di pervasività e inafferrabilità. Ogni organizzazione, infrastruttura interconnessa, servizio o applicazione digitale è un potenziale bersaglio per aggressori che possono agire nell'ombra, anonimamente, e da distanze che sono un problema solo per le forze di sicurezza condizionate dai confini nazionali. La *cyberwar* svincola dai territori, consente ai reparti *cyber* e ai loro accoliti di agire al di fuori dei propri confini. Più la nostra vita diventa iperstorica, cioè dipendente dalle infrastrutture e dai servizi digitali, più siamo esposti e vulnerabili agli attacchi *cyber*. Quindi, il fatto che l'Ucraina non sia ancora un Paese altamente digitalizzato costituisce un aspetto positivo. La Russia è molto più a rischio.

Al momento, gli effetti degli attacchi *cyber* russi sono stati la violazione di molti siti, la grande attività di disinformazione, l'interruzione di alcune comunicazioni, e la chiusura di alcune piattaforme e di alcuni *social network*. La Russia impone filtri e blocchi e cerca di controllare informazioni e comunicazioni. Si difende investendo nel proprio sistema elettronico per i trasferimenti bancari (lo Spsf), dato che il sistema internazionale Swift è stato sospeso, e in un sistema di carta di credito cinese (UnionPay), perché American Express, Mastercard e Visa hanno sospeso i loro servizi.

I potenziali protagonisti della guerra digitale hanno schierato le proprie forze. Anonymous ha dichiarato di sostenere l'Ucraina; il governo di Kiev ha lanciato un appello per la costituzione di una *It army* che possa sostenerlo; mentre la Russia ha storici fiancheggiatori nel crimine organizzato e rafforza la sua strategia di costruire una rete sovrana nazionale, svincolandosi dalle "pericolose" influenze del mondo libero. Anche in questo la Cina è stata antesignana: il Golden shield project e il Great firewall che separa la sua Internet dal resto del mondo esistono da più di vent'anni.

Tutto questo colpisce la potenzialità di esprimersi *online*, la capacità di essere cittadini del mondo anche digitali, secondo quello che fino a ieri era il normale svolgersi della vita *onlife*, cioè sia *online* sia *offline*. Tuttavia, la *cyberwar* si muove ancora secondo canoni noti. Per fortuna, non ha quelle caratteristiche distruttive e letali che si temono. Purtroppo, ciò potrebbe cambiare quando l'interconnessione tra mondo fisico e digitale sarà completata e se il controllo delle armi sarà automatizzato senza misure di sicurezza, dato che i sistemi di intelligenza artificiale sono vulnerabili come qualsiasi prodotto digitale. Ma non ancora in questa guerra, non in territori tecnologicamente immaturi, e non con questi protagonisti. Si tratta di una guerra ibrida, con attacchi *cyber* ma non ancora una vera *cyberwar*, in cui l'arma digitale è temibile per i disservizi che può causare, non per la sua potenziale violenza distruttrice.

Molto più elevato è il rischio di escalation di attacchi *cyber* non limitati alle parti in conflitto, ma estesi a altri Paesi. Probabilmente Putin reagirà alle sanzioni e alla fornitura di armi da parte dell'Occidente anche con attacchi *cyber* meno compromettenti per l'attore, quasi impossibili da attribuire con certezza giuridica o diplomatica, ed estremamente efficaci se lanciati contro Paesi altamente interconnessi e maturi digitalmente. Inoltre, gli attacchi condotti mediante *software* malevoli, analogamente ai virus biologici, non si fermano ai confini e i precedenti sono molto gravi. Dopo l'annessione della Crimea nel 2014, nell'inverno del 2015-2016 un massiccio attacco informatico tramite il *malware* BlackEnergy lasciò centinaia di migliaia di ucraini senza energia elettrica e riscaldamento. Nel 2017, a supporto della "diplomazia coercitiva", molte aziende e

Il Sole 24 ORE

Data: 17.03.2022 Pag.: 17
Size: 413 cm2 AVE: € 54103.00
Tiratura: 91744
Diffusione: 138603
Lettori: 713000

infrastrutture critiche ucraine furono sabotate mediante i *malware* NotPetya e Bad Rabbit, con effetti a catena in tutto il mondo, Russia compresa. Aziende come Maersk, Merck, FedEx-Tnt, Saint-Gobain, Mondelēz furono bloccate per giorni con danni stimati in dieci miliardi di dollari: l'attacco più costoso della breve storia *cyber*. A gennaio, il *malware* WhisperGate ha infiltrato diverse organizzazioni ucraine. A febbraio, HermeticWiper ha attaccato i sistemi commerciali e governativi del Paese.

Anche in Italia, le infrastrutture critiche nazionali sono in allerta. La raccomandazione per tutte le imprese, gli enti, e le stesse persone è tenere l'attenzione molto alta e applicare tutte le misure di protezione, a partire da *firewall*, antivirus, frequenti *backup* dei dati e replica dei servizi. E non solo in questo periodo drammatico perché la ritorsione potrebbe avvenire fra mesi.

I grandi attori del mondo digitale, come le piattaforme e i *social*, sono restii a farsi coinvolgere e si sono limitati a ridurre in Russia i servizi che avrebbero potuto indirettamente causare danni alle persone. Sono mai disposti a favorire atti distruttivi contro infrastrutture e cittadini, e non solo per ipotetici motivi commerciali. La guerra, cinetica o *cyber*, non rientra tra gli obiettivi di queste multinazionali e ancor meno dei loro dipendenti. La verità è che l'informatica, Internet, il Web, l'Ai e in generale il digitale non nascono per attaccare e distruggere, ma per proteggere e costruire. Forse una buona notizia in questo travagliato inizio del nuovo decennio è che l'Europa finalmente acceleri la realizzazione di una strategia comune di difesa informatica, che completi e rafforzi il quadro normativo europeo nell'ambito digitale. Non ce n'è mai stato tanto bisogno.

PIÙ LA NOSTRA VITA DIVENTA DIPENDENTE DA INFRASTRUTTURE E SERVIZI DIGITALI PIÙ SIAMO ESPOSTI E VULNERABILI AGLI ATTACCHI CYBER