L'Edicola del Sud
www.ledicoladelsud.it
domenica 13 marzo 2022
BARI
€1,50 € 1,00 Italia - Anno 2 / Numero 71

DIRITTO & ECONOMIA

I RISCHI DELLA (NUOVA) GUERRA CI CONSOLA SAPERE CHE, ANCHE DA QUESTA PARTE, CI SONO GRANDI ESPERTI

Con i cyber attacchi si riscrivono le regole

Il prof. Robert Tappan Morris è un quasi sessantenne ancora molto giovanile. Insegna al Massachusetts Institute of Technology, MIT: una delle più importanti università di ricerca del mondo. Il prof. Morris è anche un imprenditore di successo: ha prima fondato e poi venduto a caro prezzo una piattaforma per la creazione di siti di e-commerce. In soli tre anni è diventato milionario (in milioni di dollari). Nel curriculum del prof. Robert Tappan Morris compare però una parola: hacker. Già, il nostro amico Robert, ancora prima di diventare professore e milionario (in dollari), è stato (non sappiamo se lo sia tuttora), un hacker. E su quella mitologica, per gli amanti del genere, impresa, ha costruito la carriera. Grazie ad un verme (proprio così, "worm" battezzò il suo primo programma) in poche ore il giovane Robert, non ancora professore e milionario, ma certamente hacker, riuscì ad infettare migliaia di computer. Il vermicello discreto, occupava infatti poco spazio nelle memorie dei pc, era alquanto vivace e si replicava velocemente grazie ai contatti con i computer, infettandoli tutti. Quanto Robert fu scoperto gli venne riconosciuta la buona fede e, diciamolo pure, la superficialità comune in quella fascia di età. Comunque la Giustizia gli fece pagare un prezzo. Perché la storia del prof. Morris oggi è così importante? Perché dimostrò due cose: la prima è che nessun sistema informatico è inviolabile. La seconda è che anche le azioni di un ragazzo sveglio e bravo con il computer, avrebbero potuto generare danni incalcolabili (che fortunatamente quella volta non si verificarono). Da quell'epoca romantica ad oggi sono stati fatti molti passi in avanti (o indietro a seconda dei punti di vista) e anche molti danni (in parte rimediati). Il diffondersi della tecnologia ad ogni livello ha dimostrato una terza cosa, che all'epoca il giovane Robert probabilmente poteva solo intuire: non c'è vicenda umana che non sia toccata dal rischio, reale o teorico, di essere violata da un cyber attacco. Dai sospetti di attacchi hacker alle ultime elezioni presidenziali americane al furto di dati sanitari di una importante regione italiana. Nessuno ne è immune. E questi attacchi possono diventare facilmente armi belliche. Prima ancora che la tragica vicenda dell'invasione russa dell'Ucraina assumesse le dimensioni che stiamo conoscendo, hanno fatto scalpore le dichiarazioni di Anonymous e le azioni dimostrative poste in essere. Cosa dobbiamo aspettarci dalla guerra in atto sotto il profilo dei cyber attacchi? Potrebbero essere presi di mira, e quindi distrutti o rubati, i nostri dati bancari, i nostri depositi, o i complessi sistemi informatizzati che assicurano il funzionamento di grandi e piccole aziende? Molto più semplicemente: potrebbe essere hackerato il pc di casa o violato il mio conto corrente? Anche in questo caso la storia ci aiuta e ci offre una chiave di lettura di come la guerra, pur senza colpirci fisicamente con le armi che stiamo imparando a conoscere (ed è già tanto), potrebbe colpirci con armi telematiche. Ne sa qualcosa una delle principali compagnie di assicurazioni del mondo, che solo qualche mese fa (quindi se volete in tempo di pace) ha subito un attacco con il furto di documenti dai propri archivi. Tutti hanno avuto i loro problemi: da noti marchi automobilistici ad aziende produttrici di consolle di videogames. L'industria quindi, potrebbe essere facilmente attaccata. E' già successo. Nessuno può escludere che non accadrà ancora. E le banche? E i nostri soldi? Nella seconda metà degli anni duemila, alcuni hacker ucraini e russi, questa volta uniti, sottrassero circa 160 milioni di dati connessi alle carte di credito e 800 mila credenziali di accesso ai conti correnti. Sotto attacco finirono due delle più famose società al mondo di carte di credito. Sembra, ma certe cose è bene non dirle in giro, che la BCE, la banca Centrale Europea presieduta da Christine Lagarde, abbia invitato le banche dell'eurozona a saggiare la resilienza finanziaria dei propri sistemi da attacchi informatici. E noi? Cosa possiamo fare per difenderci ? Come individui molto poco, o meglio adottare le basiche norme di prudenza che però, sia ben chiaro, di fronte ad un attacco informatico possono assicurare lo stesso grado di resistenza di un guscio d'uovo su cui passano i cingoli di un carro armati. Non c'è password pazientemente costruita con "nomefiglio+datadinascita+*" (usiamo tutti le stesse tecniche, tra noi possiamo dircelo) che possa reggere l'onda d'urto di un attacco informatico. Dobbiamo essere preoccupati? Certamente, come sempre, come ogni giorno. In tempo di pace ed in tempo di guerra. Ormai la tecnologia governa ogni aspetto della nostra vita, dal più semplice al più complesso. Tutto, a partire dalla applicazione per l'acquisto di cibo a domicilio per finire al sistema di controllo degli aerei su cui viaggiamo, passa attraverso i sistemi informatici. Anche i nostri stipendi, i nostri investimenti, i nostri soldi. Ci consola sapere però che, anche da questa parte, nella difesa dai cyberattacchi, ci sono molti moderni prof. Robert Tappan Morris pronti a combattere per noi.

MASSIMO MELPIGNANO

Non c'è vicenda umana che non sia toccata dal rischio di essere violata da un cyber attacco

Trasporti e Logistica:	+108,7%
Professional, Scientific, Technical:	+85,2%
News & Multimedia:	+65,2%
Retail:	+61,3%
Manufacturing:	+46,9%
Energia / Utilities:	+46,2%
Governativo / Difesa:	+39,2%
Arte e Divertimento:	+36,8%
Sanità:	+18,8%

RAPPORTO CLUSIT Nel 2021 sono aumentati gli attacchi

Alcuni hacker ucraini e russi, questa volta uniti, sottrassero 160 milioni di dati connessi alle carte di credito

Massimo Melpignano
avvocato specializzato in diritto bancario