**Chiacchiere sulla (cyber) sicurezza**

Nel nostro paese, negli ultimi anni, è aumentato considerevolmente l’utilizzo di parole composte in cui primo termine è “cyber” (cybersecurity, cyberstrategia, cyberspace) utilizzate in riferimento  alla gestione delle informazioni tramite sistemi elaborativi e alle reti di interconnessione.

Questo proliferare di agenzie governative, rapporti e relazioni al parlamento, gruppi di lavoro e normative ad hoc dovrebbe ingenerare nell’opinione pubblica la presunzione che la sicurezza delle informazioni (o cybersecurity secondo la moda del momento) sia un argomento vivo, sentitoche rivesta un ruolo di primo piano nelle agende, tanto business, quanto governative. Il successivo pensiero dovrebbe logicamente essere, “ …*se molti sono sensibili all’argomento allora sicuramente si starà facendo molto…* “ e , soprattutto, la serena convinzione che una tale moltitudine di iniziative afferisca ad una strategia complessiva ben strutturata ed accuratamente pianificata.

Da addetto ai lavori, purtroppo, non ho elementi per verificare se vi sia solo una politica mediatica volta, tra l’altro, a tranquillizzare i cittadini o semplicemente, come troppo spesso accade nel campo della prevenzione, se le moltissime, e buone, intenzioni sono destinate a rimanere tali e ad essere seguite da pochissimi, e discutibili fatti.

Infatti, considerando che, a livello nazionale, la prima “Relazione sulla politica dell’informazione per la sicurezza” è stata presentata in parlamento nel 2007 (sorvolando, momentaneamente, sul fatto che negli USA la prima norma sulla cybersecurity è stata emanata nel 1987), sarebbe plausibile attendersi, tanto dal settore pubblico quanto da quello privato, un adeguato impegno relativamente alla protezione dei sistemi elaborativi.

Il settore pubblico, da un lato, ha il dovere di proteggere le informazioni dei cittadini anche a garanzia dei moltissimi (forse tutti) servizi che non possono essere erogati senza il supporto della componente tecnologica. Il settore privato, dall’altro, dovrebbe avere un interesse primario a difendere la sua operatività, il suo business, la sua capacità di restare sul mercato: elementi ormai indissolubilmente legati all’efficienza dei sistemi informativi e alla capacità di scambiare informazioni in maniera rapida ed efficiente.

Ma allora, è legittimo chiedersi, perché stiamo perdendo la silenziosa guerra contro i nuovi criminali della rete?

Le informazioni che arrivano da fonti autorevoli, infatti, disegnano uno scenario attuale per nulla rassicurante e che non lascia ben sperare nell’immediato futuro. Secondo il recente rapporto del CLUSIT, la più importante associazione nazionale che ha l’obiettivo di “*Promuovere e diffondere nel nostro paese la cultura e la consapevolezza della sicurezza informatica in tutti i suoi aspetti, in collaborazione alle consociate associazioni europee*”, l’Italia è ormai entrata nella poco invidiabile classifica delle dieci nazioni con il più alto numero di vittime da reati informatici.

Certamente questo triste primato è stato fortemente agevolato dalla massiva diffusione del cosiddetto “ransomware” ovvero una specifica tipologia di attacco informatico dove l’attaccante, tramite un apposito programma solitamente allegato ad una mail fittizia, riesce a cifrare tutti i dati del computer attaccato e chiede una somma di denaro in cambio della chiave per decifrare. Malgrado il “riscatto”, ransom in inglese, molto spesso non superi singolarmente i 200 dollari, secondo l’analisi, prudenziale, effettuata da  Herjavec Group, azienda operante nel settore della cybersecurity dal 2003, nel 2016 il suo costo complessivo non e stato inferiore al miliardo di dollari.

Ma questi dati sono solo la punta dell’iceberg. Il crimine informatico, obiettivamente, è molto meno rischioso di quello tradizionale e, generalmente, molto più redditizio. Per questa ragione si assiste ad una sua continua evoluzione, con obiettivi diversi a seconda delle capacità di questa nuova generazione di delinquenti. Sempre il rapporto CLUSIT riporta che gli attacchi verso le infrastrutture critiche del nostro paese (ospedali, centri di distribuzione dell’energia, acquedotti etc.) sono più che abbondantemente raddoppiati nell’ultimo anno. Le ragioni per cui un hacker cerchi di prendere il controllo di un ospedale sono sostanzialmente due: la prima, la più ovvia, chiedere un riscatto minacciando di spegnere tutti i sistemi informativi; la seconda, sicuramente più preoccupante, è quella di cederne il controllo a criminali “comuni” che vogliano mettere in atto azioni dimostrative.

Alla luce di questi dati è più che legittimo domandarsi perché nonostante, secondo Bankitalia, il 45% delle aziende sia stata vittima degli hacker ad oggi, stima Eurispes, solo il 19% di esse ha messo in campo progetti concreti e vision a lungo termine?

Perché le imprese nazionali sono disposte, in tempi di crisi economica, a perdere almeno 9 miliardi di euro in seguito ad attacchi informatici (fonte Eurispes)?

A queste domande ha provato, in qualche modo, a rispondere la società Ernst&Young con il suo annuale rapporto, giunto ormai alla diciannovesima edizione, dedicato all’information security ~~(o cybersecurity se vogliamo seguire la moda del momento)~~, e che viene redatto dopo aver intervistato oltre 1350 manager in tutto il mondo.

I dati del rapporto presentano un mondo aziendale con una bassa consapevolezza del problema. Infatti, a fronte di quasi 6 manager su 10 (57%) che dichiarano di aver avuto eventi significativi nell’ambito della cybersecurity, meno di 4 su 10 (36%) ha un piano strutturato su come affrontare questa problematica. L’unico ambito su cui quasi tutti concordano (86%) è che il personale impiegato non è in grado di soddisfare le esigenze aziendali.

In conclusione, possiamo dire che si parla e scrive moltissimo di cybersecurity ma, paradossalmente, l’interpretazione dei dati raccolti va ben oltre le versioni ufficiali. La percezione è che la sicurezza delle informazioni non venga realmente percepita, né come un esigenza concreta né, tantomeno, come una disciplina a sé stante, che richiede competenze specifiche. Sulla ragione di questo atteggiamento si possono solo avanzare ipotesi. Quella verso la quale sono portato a propendere è legata al fatto che la sicurezza lavora sulla prevenzione, sull’immaginare qualcosa che deve ancora accadere. Il suo ritorno economico è stimato in base ad una potenziale mancata perdita. E’ priva di materialità al punto tale che il manager tradizionale, abituato ad avere a che fare con fatturati e dati di produzione, non ne percepisce concretamente la stringenza sino a quando non è troppo tardi.

Per questo, ripeto spesso che lavorare nel campo della cybersecurity è un lavoro maledettamente strano: finché non succede nulla sei pleonastico, in quanto la tua figura è solo un costo per l’azienda fino a quando non succede qualcosa (magari perché l’azienda ti ha negato il budget per l’implementazione dei sistemi di sicurezza) ed allora diventi istantaneamente un incompetente, per non aver gestito la situazione con sufficiente lungimiranza ed efficacia.