Il Sole 24 ORE
Dir. Resp.: Guido Gentili
07-MAR-2018
da pag. 10
foglio 1
www.datastampa.it
Tiratura: 141860 - Diffusione: 187721 - Lettori: 803000: da enti certificatori o autocertificati
Superficie: 17 %

Nell'era dei dati / 2. Per prevenire e gestire gli attacchi al patrimonio digitale è necessaria la cooperazione tra le aziende

La sicurezza è una questione di «filiera»

di **Giorgio Mosca**

La trasformazione digitale è al centro dello sviluppo economico dell'Europa da ormai quasi 20 anni. Essendo il settore digitale in rapidissima e costante trasformazione quest'attenzione ha più volte trovato nomi e canali diversi per farsi strada nell'agenda politica europea, dall'economia della conoscenza, all'agenda digitale, al Digital single market, all'Industria 4.0.

Con il piano Impresa 4.0, anche l'Italia ha riconosciuto la necessità di accelerare la trasformazione digitale delle attività economiche come fattore di competitività, produttività e sviluppo. In questo senso le misure introdotte dal governo e le iniziative territoriali di creazione e diffusione della conoscenza sul tema (ad esempio la rete dei Digital innovation hub e la creazione dei Centri di competenza ad alta specializzazione) sono azioni che vanno nella giusta direzione di aiutare le imprese nazionali, spesso piccole e non attrezzate per comprendere opportunità e vincoli di una digitalizzazione spinta, a trovare una propria strada verso l'innovazione digitale.

In questo positivo quadro di attenzione allo sviluppo digitale è però fondamentale non trascurare l'importanza rivestita dalla *cyber security* (ovvero la protezione dei processi e delle informazioni digitali) e dalla *cyber resilience* (ovvero la capacità dei sistemi digitali di garantire l'operatività in presenza di anomalie).

Le aziende, gli enti di standardizzazione e le istituzioni hanno dedicato decenni a sviluppare quelle logiche di protezione e sicurezza che costituiscono ciò che in termini anglosassoni è chiamata "*safety*" e che sono ormai implementate in tutti i sistemi di controllo industriale. Lo stesso processo deve ora essere realizzato, in ottica Industria 4.0, per implementare logiche di protezione e sicurezza digitali, cioè per quelle aree che in termini anglosassoni vengono definite "*security*" e "*resilience*". A differenza di quanto accaduto in precedenza però non abbiamo decenni per realizzare queste soluzioni e non possiamo farlo macchina per macchina e impianto per impianto; il presupposto della digitalizzazione è l'integrazione di macchinari, sistemi e impianti, che si estende al di fuori del sito produttivo o della singola impresa, e viene aggiornata e modificata non nell'arco di anni, ma di giorni se non addirittura di ore.

Questa dinamica completamente differente rispetto alle attività delle imprese prima della quarta rivoluzione industriale, pone in evidenza alcune necessità fondamentali:

- le imprese devono collaborare tra di loro non solo per il business, ma per la protezione dello stesso; non esisteranno più clienti e fornitori che si scambiano informazioni occasionalmente, ma solo partner di una filiera produttiva digitalmente integrata, che deve essere protetta *in toto* poiché sarà tanto resistente quanto il suo anello più debole;
- le aziende di maggiore dimensione devono farsi promotrici di iniziative di sensibilizzazione, di formazione e di costruzione di capacità di sicurezza e resilienza nella propria filiera, anche in Italia come già accade in altri Paesi europei più avanzati in questo processo;
- le istituzioni e le associazioni devono dare il proprio contributo operando in vera sinergia e creando le condizioni per la costituzione di una domanda aggregata di *cyber security*, basata su un modello condiviso di comportamento, che possa stimolare un'offerta adeguata per il tipo di tessuto imprenditoriale nazionale;
- gli enti formativi (scuole, Its, università) devono fare la loro parte, formando le professionalità necessarie per supportare le imprese nazionali nello sviluppo di digitalizzazione e sicurezza cibernetica.

Il tempo di agire è ora. Tutti devono comprendere che è necessario dare una risposta unitaria alla domanda di cyber sicurezza che la trasformazione digitale ci pone e che si deve darla subito.

Le istituzioni nazionali hanno lanciato , con il Dpcm Gentiloni dello scorso febbraio e la nuova strategia nazionale, un segnale di attenzione e di capacità di comprendere le dinamiche del settore; l'adozione di direttiva Nis e regolamento Gdpr daranno un ulteriore impulso, come pure la spinta verso la certificazione promossa dalla Commissione europea. Anche altri *stakeholder* stanno contribuendo, ad esempio il Laboratorio nazionale di *cybersecurity* con Rapporti e Libri bianchi, Banca d'Italia con la sua indagine specifica, Confindustria Digitale con i *roadshow* nelle principali località italiane.

La costruzione di filiere digitalmente integrate potrà avere successo, senza esporre il tessuto economico nazionale a nuovi e maggiori rischi, solo se la protezione dei flussi informativi e finanziari, dei processi produttivi e della proprietà intellettuale, sarà considerata parte integrante della costruzione di un modello italiano di Impresa 4.0. Questo modello dovrà tenere conto del fatto che molte Pmi hanno un enorme patrimonio di competenze e capacità professionali specialistiche nel proprio settore di eccellenza, ma non nell'ambito dei sistemi informatizzati. Per una Pmi è in genere impossibile dotarsi di risorse interne dedicate alla digitalizzazione o alla *cyber security*. I servizi di sicurezza potrebbero quindi far parte di un approccio condiviso, ad esempio all'interno di un settore o di una filiera, e addirittura essere messi a fattore comune promuovendo l'aggregazione attraverso il meccanismo delle "Reti d'impresa".

Presidente Steering Committee Cybersecurity di Confindustria Digitale