Relazione Riunione del Gruppo di Riflessione COTEC

<u>Oggetto</u>: "Protocollo *cybersecurity* per le PMI / Modello organizzativo, strategico e procedurale"

07 Marzo 2019, Link Campus University

Si è avviata la riflessione sulla proposta di elaborare un modello strategico, organizzativo e gestionale per le piccole-medie imprese (PMI) nell'affrontare il tema della *cyber security,* i cui risultati sono qui di seguito sintetizzati.

Obiettivo

Con l'obiettivo l'intento di promuovere una appropriata cultura aziendale in materia di sicurezza cibernetica, il modello proposto mira allo sviluppo di strutture organizzative sicure e preparate a fronteggiare possibili attacchi interni ed esterni, ad evitare i rischi e ad adottare modalità strategiche e strumenti di prevenzione e tutela a protezione dei dati sensibili di ogni impresa. La peculiarità dell'iniziativa riguarda l'affiancamento e il supporto delle grandi imprese alle PMI; queste ultime non risultano in generale in grado di sostenere attività strategiche di protezione informatica e, pertanto, necessitano dell'*expertise* delle prime. Grazie alla definizione di un protocollo *di cyber-security*, quindi, le grandi aziende possono offrire una serie di servizi, ovvero un *cyber range services*, alle PMI, permettendo così di mitigare i rischi e ridurre la superficie di attacco cibernetico.

Il Protocollo

Il *Protocollo di Cyber-Security per le PMI*, definito come strumento di autovalutazione e *self-report*, permette di avviare un processo di formazione delle PMI fornendo loro le linee guida da seguire, e allo stesso tempo consente di qualificare anche tutti coloro che forniscono i *cyber range services*. In questo modo, le PMI, destinatario della formazione, possono raggiungere un'adeguata preparazione di fronte a rischi d'attacco; mentre le grandi imprese svolgono il ruolo di formatori condividendo il loro *expertise*. Per entrambi i soggetti, l'obiettivo finale è quello di rafforzare e rendere competitivo in termini di sicurezza tutto il sistema produttivo.

In questo contesto il Gruppo di Riflessione COTEC intende elaborare le linee guida da adottare, con la possibilità di presentarle al Governo e attivare un processo legislativo (tramite decreto ministeriale) per la codifica normativa del protocollo stesso. Quest'ultima iniziativa, però, richiede molto tempo; pertanto, si ritiene più produttivo concentrarsi sull'acquisire ampia adesione delle PMI al sistema di linee guida di carattere volontario e non vincolante.

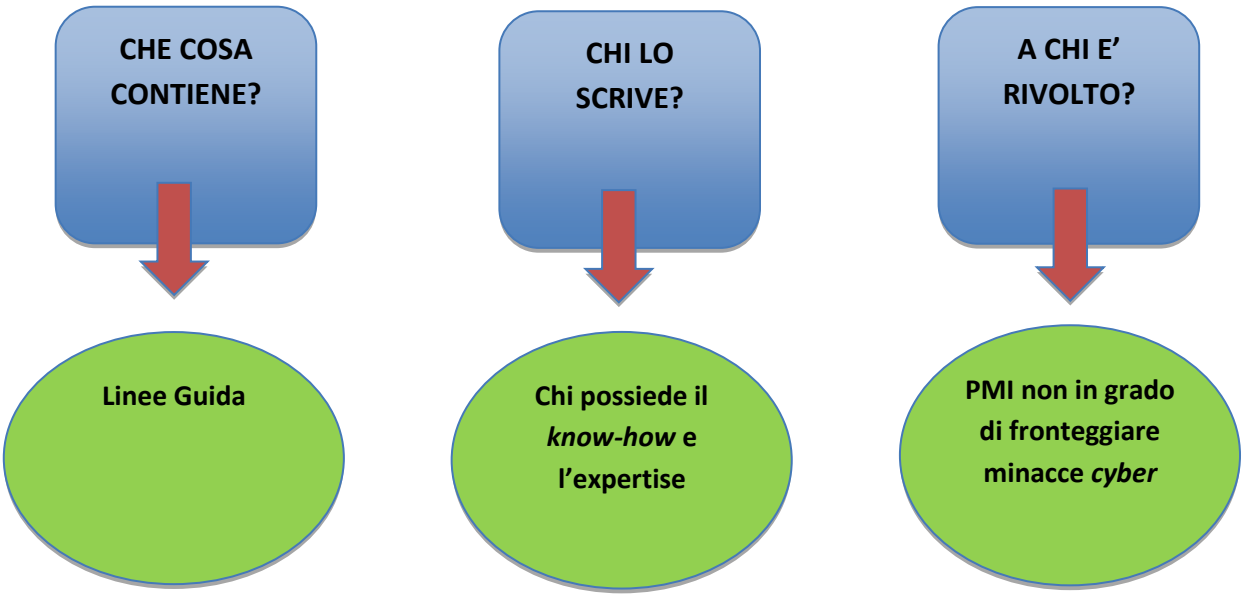
Innanzitutto, la stesura delle suddette linee guida dovrà, considerare come punto di partenza le già esistenti raccomandazioni nazionali. Di conseguenza, dando per note le linee nazionali sarà necessario contestualizzare nel dettaglio specificando l'elemento aggiuntivo offerto dal Protocollo

di *cyber-security*: un *insight* rivolto al supporto di una crescita di consapevolezza, di cultura e di opportunità per le PMI distribuite su tutto il territorio italiano. Inoltre, ogni PMI sarà stimolata a seguire le indicazioni fornite dalle linee guida per propria volontà al fine di assicurarsi sui possibili rischi cibernetici a cui potrebbero essere soggette. Non si tratta, dunque, di seguire prescrizioni obbligatorie, ma di una autonoma decisione di una PMI nel provvedere ad accrescere la propria sicurezza.

Un'ulteriore riflessione sull'essenza stessa del protocollo rimanda al fatto che a prescindere da questa adesione, auspicabilmente positiva, di numerose PMI, rimane l'esposizione al rischio cibernetico. Pertanto, si è evidenziato come possa risultare necessario intendere il protocollo anche come un contributo all'autovalutazione di ciascun imprenditore per la propria impresa. Considerando anche questo aspetto, nel tentativo di mitigare il rischio cibernetico a cui le PMI sono esposte, bisogna anche offrire un contributo operativo tale da permettere loro di valutare la propria esposizione o meno a questo rischio. Inoltre, nella misura in cui questi *standard* risultino efficaci ed efficienti, potranno anche essere acquisiti dalla Pubblica Amministrazione e dalle grandi imprese come criterio proprio di valutazione dell'adeguatezza di questo modello di fornitura di nozioni guida nel trasmettere strumenti di contrasto agli attacchi informatici.

Nell'ottica di ridurre il rischio cibernetico per tutte le PMI italiane attraverso un'operazione di formazione, informazione e sensibilizzazione, l'istituzione di linee guida rappresenta anche un tentativo di contrapposizione al *cloud* nazionale. Infatti, in alternativa ad avere un insieme di soggetti che singolarmente e autonomamente si offrono per gestire e assicurare i dati delle PMI, la presenza di linee guida specifiche e adottate da tutte queste ultime mira a portare in qualche modo tutte le stesse PMI ad avere comportamenti omogenei. Di conseguenza, le grandi imprese, i Comuni e le Pubblica Amministrazioni sono stimolate a promuovere la diffusione di queste linee guida. Inoltre, si propone di invitare tramite un documento di raccomandazioni alle Pubbliche Amministrazioni a considerare come fattore premiante tutte le PMI che hanno scelto di adottare operativamente le linee guida.

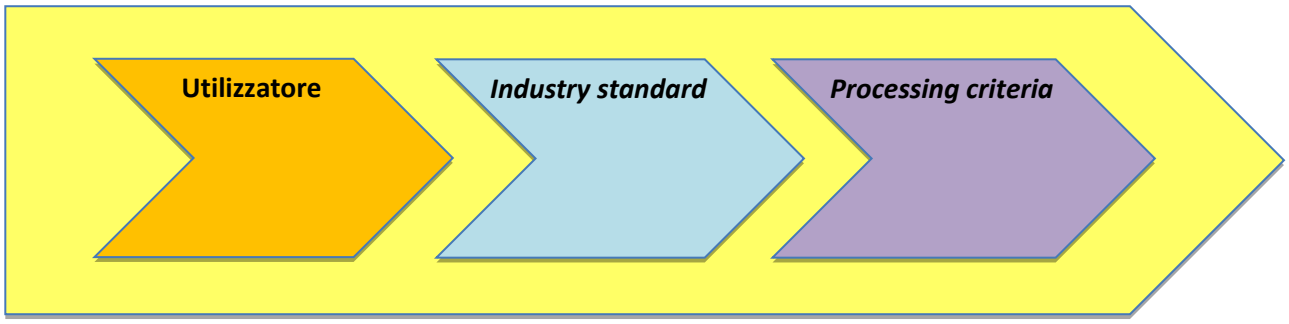
Protocollo in sintesi



Il Protocollo viene per semplicità visto come un processo a molti stadi, suddiviso in tre "stadi" ciascuno dei quali tratta un elemento caratterizzante rivolto all'obiettivo generale ovvero arrivare ad un autovalutazione dell'impresa per quanto riguarda la sicurezza cyber, che è volontaria e rivolta a tutti.

Gli elementi caratterizzanti sono:

a. Utente: amministratore delegato della PMI;
b. *Industry standard*: linee guida a cui le aziende possono aderire volontariamente e nel momento in cui aderiscono comunicano all'esterno che stanno rispettando quei criteri;
c. *Processing criteria*: premio chi aderisce in maniera volontaria alle *industry* standard;



Il modello proposto considera come elemento prioritario coloro che hanno effettiva necessità di monitorare la sicurezza *cyber*, cioè le aziende che lavorano per la Pubblica Amministrazione, direttamente o attraverso le imprese sistemiste nazionali, e che quindi soffrono maggiormente l'assetto strutturale se non soggetti di un sistema di controllo *cyber* che si gestiscono autonomamente.

Prossimi Passi

In base alle considerazioni precedentemente delineate si sono definite le attività da svolgere finalizzate ai seguenti obiettivi:

- Ridurre i rischi della superficie d'attacco: le PMI sono i principali soggetti che fanno aumentare la superficie d'attacco e che, quindi, rischiano di essere gli *entry point* dell'infezione cibernetica;
- Elaborare le linee guida e le modalità di autovalutazione che consentono di creare avvertenza nel piccolo imprenditore;
- Diffondere informazioni e acquisire consenso sul Protocollo, sulla base di volontarietà e convenienza all'adozione di linee guida per difendere il patrimonio aziendale e contribuire al generale interesse.

Sulla base di questi propositi, i prossimi passi consistono:

a) nell'organizzare un incontro con le associazioni delle PMI per proporre il Protocollo allo scopo di comprendere le loro valutazioni e indicazioni e acquisire consenso attorno ad esso. Un possibile approccio per affrontare tale problematiche con le PMI può essere fare riferimento al rapporto *Clusit* per avere un quadro sugli incidenti informatici legati alle PMI. Considerandol'impatto sia quantitativo sia qualitativo: cioè non solo l'aumento del numero degli incidenti, ma anche l'aumento del danno.
b) Procedere con la stesura delle linee guida.

Infine, da ultime sono emerse alcune considerazioni per ulteriori sviluppi del lavoro del *Cyber*:

- Valutare l'impatto dell'Intelligenza Artificiale sulle PMI;
- Considerare il mondo delle *Start Up* e suggerire loro l'adozione delle linee guida;
- Approfondire l'aspetto della "Fabbrica Intelligente", quale modello di riferimento per le PMI, il cui dilemma consiste nel rischio di interventi *pro-cybersecurity* ma dannosi per l'impresa stessa, provocando una chiusura alla tecnologia e perdendo così anche competitività nel mercato.