FRAMEWORK NAZIONALE CYBER-SECURITY

CONCLUSA LA CONSULTAZIONE PUBBLICA

Il CIS SAPIENZA (Cyber Intelligence and Information Security [www.cis.uniroma1.it]) dell'Università degli Studi di Roma "La Sapienza" ed il Consorzio Interuniversitario Nazionale per l'Informatica (CINI [www.consorzio-cini.it]) hanno pubblicato un framework nazionale di cyber security [www.cybersecurityframework.it] e si è da poco conclusa la consultazione pubblica (bozza [http://www.cybersecurityframework.it/framework-nazionale-cyber-security.pdf]). E' prevista per il **4 Febbraio** la presentazione ufficiale e la consegna del documento al governo.

CHI HA PARTECIPATO

Il documento ha richiesto diversi mesi di lavoro ed ha avuto il supporto della **Presidenza del Consiglio dei Ministri** ed ha visto la partecipazione di un alcune aziende tra cui: AON, DELOITTE, ENEL, ENI, HERMES BAY, KPMG, INTELLIUM, PWC e MICROSOFT e di un gruppo di attori istituzionali come MISE (Ministero dello Sviluppo Economico), GARANTE PRIVACY e AGID (Agenzia per l'Italia Digitale). Il testo è stato poi aperto al contributo di tutti gli operatori ed ai cittadini che hanno voluto contribuire ad emendare il Framework Nazionale all'interno di una consultazione pubblica che è terminata il 10 Gennaio. Alla fine del processo si vuole ottenere un documento altamente **condiviso tra pubblico e privato** poiché il pericolo cyber è trasversale: sono molte centinaia gli utenti che si sono registrati per scaricare il documento ed oltre 100 gli emendamenti ricevuti.

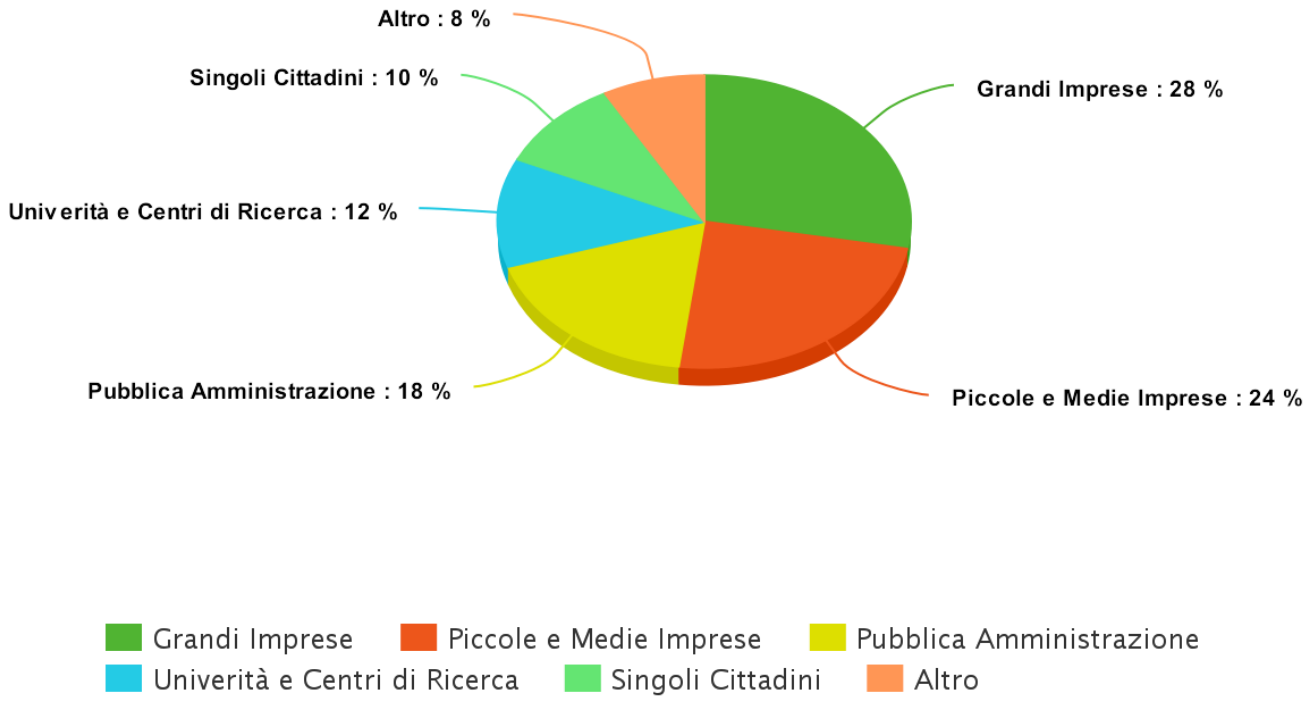

Figura 1 - Percentuale di registrazioni alla consultazione pubblica per settore

SCOPO DEL DOCUMENTO

Lo scopo del documento è quello di offrire alle organizzazioni pubbliche e private, piccole, medie e grandi, un approccio omogeneo per affrontare la cyber security, al fine di ridurre il rischio legato alla minaccia cyber. Il framework parte dal documento "Framework for Improving Critical Infrastructure Cybersecurity" [http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf] emanato (a seguito di un executive order del Presidente OBAMA per aumentare la resilienza delle infrastrutture critiche statunitensi) dal National Institute of Standards and Technology del governo americano (NIST [www.nist.gov]), ma è stato ampliato ed attualizzato al contesto italiano. Il Framework nazionale si pone infatti l'obiettivo di offrire una **guida per incrementare il livello di cyber security** per la Piccola e Media Impresa italiana ed offre raccomandazioni per il management di grandi aziende e infrastrutture critiche su come organizzare al meglio i processi di cyber security risk management.

COSA C'È SCRITTO

Il framework vuole fornire un **linguaggio comune per esprimere e classificare in maniera omogenea i rischi cyber**. Offre riferimenti documentali certi per i vari ambiti anche riferimenti ad obblighi normativi italiani, ad esempio, per le Pubbliche amministrazioni quelli riportati dal CAD (Codice dell'Amministrazione Digitale). L'approccio non è legato a standard tecnologici ma all'analisi del rischio. Nella prima parte si fa un quadro del panorama italiano, si chiariscono i concetti di base e si fornisce un guida per l'applicazione in base alla dimensione di impresa; Nella seconda parte si arriva al nocciolo del framework e si contestualizza nella realtà italiana con alcune raccomandazione per le infrastrutture critiche; Infine nella terza parte viene esposto lo scenario di applicazione, il mercato delle polizze assicurative, il contesto normativo italiano e gli aspetti pertinenti a pubbliche amministrazione e settore bancario e finanziario.

A COSA SERVE

L'adozione del framework è volontaria e permette all'organizzazione di aumentare la propria resilienza verso attacchi informatici e di proteggere le proprietà intellettuali. Il framework rappresenta una notevole operazione di **consapevolezza sulla minaccia cyber**, probabilmente la maggiore sino ad ora in Italia verso il settore pubblico e privato ed in particolare verso le alte sfere dirigenziali di queste organizzazioni, con il chiaro obiettivo di fare uscire il rischio cyber dai dipartimenti di Information Technology e di farlo sbarcare dentro i consigli di amministrazione. Per questo anche il linguaggio usato è volutamente non tecnico.

SI RIVOLGE ANCHE ALLE PICCOLE IMPRESE ITALIANE

Nel documento viene presentata come esempio una specifica contestualizzazione del framework per le Piccole Medie Imprese Italiane. Queste infatti faticano più di altre organizzazioni a valutare accuratamente il rischio che corrono non proteggendo i propri asset strategici (dati, documenti, progetti, servizi, prodotti, ecc.). La contestualizzazione fornisce i controlli di sicurezza che devono essere indirizzati ad alta priorità dalle PMI ed una guida per implementarli.

1	**Identificare una contestualizzazione del framework** Non è un regolamento da seguire ma una linea guida e potrebbe quindi essere modificata in base ai propri obiettivi e alle proprie criticità.
2	**Adottare controlli a priorità alta a livello di maturità minimo** Questo è un passo critico nell'implementazione del framework e consente di ottenere un livello base di preparazione e consapevolezza del rischio cyber.
3	**Identificare sistemi e asset critici** Consente di valutare propriamente gli impatti durante l'analisi dei rischi e di agevolare pertanto la comprensione delle effettive necessità di protezione.
4	**Analizzare il rischio e il profilo cyber attuale** Ciascuna organizzazione ha le sue peculiarità che determinano livelli di esposizione ai rischi differenti.
5	**Determinare il gap rispetto al profilo target** Definire un profilo target di protezione desiderato che costituisce la base per comparare il profilo corrente con quello desiderato per la gestione della cyber-security.
6	**Definire ed attuare piano di azione per raggiungere il profilo target** Elaborare un piano specifico per realizzare i singoli controlli del framework, secondo un piano temporale che varierà in relazione alle condizioni specifiche in cui opera la singola impresa.

Figura 2 - Passi per l'adozione del framework da parte di una piccola-media impresa

LA CYBER-POSTURA

A partire dalla contestualizzazione ogni impresa può definire il proprio profilo, cioè può vedere quante pratiche implementa nella contestualizzazione scelta. Si ha così **una fotografia della propria "postura" cyber**, uno stato dei fatti dal quale definire il proprio profilo target: dove si vuole arrivare, l'obiettivo da raggiungere. I livelli di priorità ed i livelli di maturità presenti in di ogni controllo di sicurezza aiutano a definire una roadmap per passare dal profilo attuale a quello prefissato. Non potendo comunque ridurre a zero il rischio cyber, nel documento viene descritto come una organizzazione può **assicurare il rischio residuo** creando un circolo virtuoso con istituti assicurativi che può portare ad un percorso economicamente sostenibile di rafforzamento delle difese cyber di una organizzazione in un periodo definito.

LA PUBBLICA AMMINISTRAZIONE

La pubblica amministrazione può avvantaggiarsi del framework in diversi aspetti. Ad esempio molti sono i regolatori del settore pubblico che normano la dimensione cyber:

AGID (Agenzia per l'Italia Digitale), PCM (Presidenza del Consiglio dei Ministri), Garante Privacy, MISE (Ministero dello Sviluppo Economico). Il framework definisce un terreno di gioco comune ed omogeneo diviso in 98 sottocategorie dove operare in modo coerente.

SUPPLY-CHAIN

Infine tra i vari vantaggi che un framework può portare al settore pubblico e a quello privato è l'incremento della sicurezza della catena di approvvigionamento (supply chain) di prodotti e servizi. Le organizzazioni potrebbero richiedere ai propri fornitori di avere un particolare profilo minimo: una serie di pratiche di sicurezza necessarie per trattare dati particolarmente critici oppure per poter interagire coi sistemi dell'organizzazione e così via.

PER IL BENE DEL SISTEMA PAESE

La cyber security è uno di quei settori dove non esiste differenza tra pubblico e privato e dove tutti gli attori devono **cooperare per il bene del sistema paese e delle singole organizzazioni**. Nessuno può affrontare il problema in isolamento, per cooperare in modo efficace abbiamo bisogno in questo delicato settore di un quadro di riferimento comune e di una lingua comune: il Framework Nazionale rappresenta questo ambizioso obiettivo.

FABIO DE PAOLIS

Fabio De Paolis è esperto in sicurezza informatica con oltre 20 anni di attività nel settore. E' laureato in Sicurezza dei Sistemi e delle Reti Informatiche presso l'Università di Milano; è CERTIFIED ETHICAL HACKER presso EC COUNCIL di Londra; è CHIEF INFORMATION SECURITY OFFICER in un'azienda italiana che offre servizi di ingegneria del software e sicurezza informatica; è consulente di enti ed organizzazioni private per individuare ed esaminare minacce informatiche; si interessa di cyber-security e cyber-warfare con particolare attenzione al mondo dell'intelligence; è attivo sulla Rete da quando la posta elettronica si scambiava solo fra BBS tramite modem analogico.