LUISS SCHOOL OF GOVERNMENT

Cybersecurity nella Pubblica Amministrazione

Policy paper 2017

Con il patrocinio di Agenzia per l'Italia Digitale (AgID), nel 2016, la Luiss School of Government ha organizzato il corso executive "Rivoluzione Digitale e Cybersecurity" rivolto ad un ristretto gruppo di dirigenti pubblici con responsabilità di sicurezza informatica nelle amministrazioni centrali dello Stato. Il progetto si è svolto grazie alla collaborazione con alcune aziende leader del settore: BV Tech, Leonardo (ex Finmeccanica), IDS, Microsoft e Unipol.

Oltre a favorire la formazione dei dirigenti pubblici da parte di esperti, il valore del corso si è concretizzato nell'offrire un inedito luogo di confronto per lo scambio di esperienze tra i partecipanti stessi. L'approfondimento di tematiche legate alla rivoluzione digitale ha permesso dunque di avviare un dialogo costruttivo tra i vari stakeholder su quelli che sono i rischi cibernetici per la pubblica amministrazione e le strategie da mettere in campo per fronteggiare tali pericoli.

Proprio in questo spirito di condivisione di problematiche e migliori pratiche il presente policy paper intende contribuire alla discussione in corso a livello nazionale sulla cybersecurity all'interno della Pubblica Amministrazione (PA). Questo documento si pone come un ragionato tentativo di contribuire al dialogo fra partnership pubblica e privata all'interno degli sforzi nazionali ed europei per preparare gli Stati a fronteggiare nuovi attacchi cibernetici, sia aumentando la resilienza delle istituzioni pubbliche, sia rafforzando la competitività nel settore privato nel suo partenariato con il settore pubblico.

Importante è sottolineare che il percorso di digitalizzazione della PA per conto di AgID rientra nel ben più ampio progetto dell'Agenda Digitale Europea, una delle sette iniziative faro della Strategia Horizon 2020 che si propone di migliorare il potenziale delle tecnologie dell'informazione e della comunicazione (ICT) al fine di favorire innovazione, crescita economica e progresso. Attraverso l'azione congiunta di Commissione Europea e ENISA (l'Agenzia dell'Unione Europea per Network e Information Security), l'UE si è dotata nel 2013 di una Strategia di Sicurezza Cibernetica che si prefigge la protezione dei diritti fondamentali, della libertà di espressione, dei dati personali e della privacy, rendendo lo spazio digitale accessibile a tutti e stabilendo una governance condivisa, democratica ed efficiente.

Alla luce dell'architettura istituzionale europea a riguardo e della direttiva Network and Information Security (NIS) del luglio 2016, il policy paper si articola in due sezioni. Nella prima parte si raccolgono le raccomandazioni provenienti dai dirigenti

della Pubblica Amministrazione che hanno partecipato al corso. Le criticità identificate riguardano quattro temi: i servizi digitali della Pubblica Amministrazione sia interni sia esterni, il procurement di beni e servizi digitali, e le infrastrutture. Nella seconda parte si presentano, invece, le considerazioni elaborate dalle aziende che hanno sponsorizzato il corso.

Raccomandazioni della Pubblica Amministrazione

Servizi Digitali interni della Pubblica Amministrazione

Gestione degli accessi

Le procedure di gestione degli accessi ai servizi applicativi, perlopiù analoghe tra le diverse amministrazioni, attraverso l'inserimento di login e password e solo in alcuni casi con l'utilizzo del terzo fattore di autenticazione (smartcard o altro dispositivo personale), pongono alcune serie criticità. Per quanto riguarda la fase di autenticazione si è rilevato che le password scelte dagli utenti tendono a essere deboli in quanto semplici e spesso con riferimenti personali relativi all'assegnatario del servizio informatico. Tale pratica è in grado di inficiare notevolmente la sicurezza del sistema, rendendo facilmente perscrutabili i contenuti personali di ciascun utente e fornendo un canale di accesso per attacchi più complessivi.

A tal proposito si raccomanda:

- **la definizione e l'applicazione di policy comuni inerenti alla scadenza e alla robustezza delle password, oltreché l'implementazione di controlli automatici che prevedano il rifiuto delle password non sicure;**
- **l'introduzione in alcuni settori di un software di cosiddetto SSON (Single Sign On) che armonizzi e gestisca con un'unica password sicura tutti gli accessi ad ambienti logici interni ed esterni e a tutti i dispositivi impiegati, ovvero di un sistema master per la gestione dell'identità in grado di propagare le caratteristiche di profilazione di ogni utente ai diversi servizi applicativi**
- **la differenziazione degli accessi con l'utilizzo della doppia autenticazione per alcuni servizi critici quali, per esempio, la posta certificata o le operazioni dispositive.**

Bring Your Own Device, BYOD

L'approccio ibrido che contempla l'uso sia dei dispositivi forniti dall'amministrazione, sia di quelli privati per l'accesso alle risorse d'ufficio da dispositivo può comportare una seria minaccia per la sicurezza dell'intero apparato amministrativo.

Per ridurre tali rischi si raccomanda:

- **l'adozione di software e sistemi per la messa in sicurezza degli accessi in rete da parte di dispositivi che sono al di fuori del perimetro di gestione dell'amministrazione, cioè di segregazione, degli ambienti pubblici e privati (ad. es. sistemi NAC, SSL-VPN, etc);**
- **la diffusione di linee strategiche da parte di AgID;**
- **il potenziamento in tutte le amministrazioni di iniziative formative e informative volte a sensibilizzare gli utenti dei sistemi informativi sui rischi della fruizione dei dati d'ufficio attraverso i propri canali privati.**

Si segnala inoltre la convenzione Consip per la telefonia mobile, nell'ambito della quale è offerto anche il servizio di MDM (Mobile Device Management) che permette di registrare le dotazioni informatiche dell'ambiente d'ufficio in maniera rapida, configurando e aggiornando le impostazioni dei dispositivi over-the-air e proteggendo allo stesso tempo quelli mobili. Da un'unica console di gestione è possibile così controllare tutti i dispositivi registrati di proprietà aziendale, personale o condivisa. È comunque da sottolineare la particolare criticità che caratterizza le tematiche di gestione dei mobile in accordo alle prescrizioni dell'articolo 4 Legge 300/1970, per la quale strumenti potenzialmente idonei a tracciare da remoto la prestazione del dipendente non possono essere adottati dal datore di lavoro se non tramite previo accordo con le rappresentanze sindacali.

Servizi Digitali esterni alla Pubblica Amministrazione

Sistema Pubblico di Identità Digitale, SPID

Si segnala favorevolmente l'azione della regolamentazione eIDAS per l'identificazio-

ne elettronica e i trust service per le transazioni informatiche nel mercato interno europeo. In questo senso, l'AgID ha ben saputo allinearsi alle direttive presentate dall'UE per ciò che concerne i programmi di firma e identità digitale. Nel generale apprezzamento dell'azione dell'AgID per l'allineamento alle direttive europee, nell'iniziativa SPID si riscontrano alcune lacune quali, ad esempio, la mancanza di un adeguato piano di diffusione della stessa e talune vulnerabilità dei profili di sicurezza adottati, come recentemente dimostrato e pubblicizzato. Di conseguenza, l'insufficienza di soluzioni in grado di provvedere alla messa in sicurezza dell'iniziativa deve essere colmata per rendere il progetto efficace. Per gestire queste problematiche si raccomanda quindi:

- **la formulazione di una precisa strategia nazionale che miri innanzitutto a fare chiarezza fra i cittadini, facendo conoscere il prodotto su tutto il territorio nazionale e all'interno delle stesse agenzie della PA;**
- **la definizione di un piano di diffusione che specifichi tempistiche di intervento, costi (anche a carico degli utenti finali) e modalità affinché il progetto risulti effettivamente valido;**
- **la realizzazione a breve di un piano di implementazione dei profili di sicurezza adottati con riferimento sia allo strumento, sia alla definizione e gestione dei servizi a esso correlati;**
- **l'istituzione di un numero verde per la messa in sicurezza del proprio codice SPID da poter contattare nel caso di frodi e attacchi informatici alla propria identità digitale.**

Procurement

Conforme al quarto pilastro della Strategia dell'Unione Europea per la Cybersecurity, l'Italia deve puntare alla creazione di un modello di prodotti per la sicurezza informatica, promuovendo lo sviluppo di standard elevati e ricercando certificazioni nell'area cloud computing, ma mantenendo la protezione dei dati dei cittadini.

Nuovo codice degli appalti

Il nuovo codice degli appalti pone vincoli stringenti che limitano l'efficacia dell'a-

zione delle amministrazioni. Per acquisizioni di beni e servizi per importi compresi tra € 40.000 e €134.000 o €209.000 (a seconda del tipo di Amministrazione), le PP.AA. sono tenute ad elaborare metodologie e metriche di valutazione del prodotto di interesse al fine di esperire pratiche di acquisizione (procedura negoziata ex art. 36 comma 2 lettera b) con il criterio delle offerte economicamente più vantaggiose, mediante minor prezzo o migliore rapporto qualità-prezzo a seconda dei casi. Tali operazioni da svolgersi attraverso il Mercato elettronico della PA (MePA), ove la merceologia sia presente nel MePA, sono rese complesse dall'obbligo di bandire gare per un prodotto individuato non da marca e modello, bensì da generiche caratteristiche tecniche e funzionali. L'appesantimento delle pratiche di acquisizione e il conseguente dilatarsi dei tempi necessari, già di per sé penalizzante per il settore informatico (notoriamente soggetto a variazioni ed evoluzioni molto rapide), sono incompatibili con le esigenze della missione di sicurezza informatica.

Sarebbe perciò opportuno prevedere procedure più semplici e snelle per certe tipologie di acquisti particolarmente critiche come quelle per la sicurezza ICT. Considerato che nuovi tipi di minacce e di vulnerabilità possono rapidamente manifestarsi e insistere sui sistemi e sul sistema paese, la tempestività negli approvvigionamenti e la possibilità di acquisire le soluzioni necessarie senza il rischio di ingerenze (tecnologiche e amministrative) da parte di outsider rappresentano la chiave di volta per la costruzione di presidi di sicurezza realmente efficaci.

Si suggeriscono dunque le seguenti azioni:

- **la promozione di prototipi e framework metodologici/metrici per la valutazione delle soluzioni di sicurezza (in termini di robustezza, adeguatezza ed interoperabilità, ovvero in termini di realistica infungibilità) da parte di AgID;**
- **la standandardizzazione dei diversi processi di acquisto e determinazione di modalità controllate nella dinamica fornitore-acquirente che garantiscano un livello di sicurezza cibernetica per le forniture acquistate che consenta non unicamente la conservazione dei dati, ma anche la protezione degli stessi (attualmente non garantita dalla maggior parte dei bandi di fornitura di servizi informatici che si limitano a richiedere la creazione di backup);**
- **il riconoscimento di canali preferenziali alle iniziative volte a tutelare il patrimonio informativo della Pubblica Amministrazione, tanto riguardo agli oneri economici da sostenere, quanto riguardo alla libertà di scelta che deve distinguere**

operatori di settore ai quali si richiede l'assoluta padronanza degli strumenti utilizzati;

- **l'istituzione di un sistema di rating dei fornitori riferito alla sicurezza e dunque una selezione più mirata degli stessi, invitando unicamente gli operatori economici considerati idonei a seguito di tale valutazione a presentare offerte in merito;**
- **l'esecuzione di audit di sicurezza e di test delle vulnerabilità da parte di organismi indipendenti in grado di certificare la sicurezza dei sistemi ICT, con la possibilità di risolvere il contratto nel caso di falle nella sicurezza cui il produttore non riesca a porre rimedio.**

Infrastrutture

Centro Elaborazione Dati, CED

Per quanto concerne l'argomento Centri Elaborazione Dati, si osservano a livello di sistema paese gravi frammentazioni e disomogeneità nelle soluzioni logistiche, tecnologiche ed organizzative adottate per l'esercizio dei servizi informatici. Nello specifico, a livello tecnologico e logistico si lamentano gravi disomogeneità, debolezze e obsolescenze dell'informatica, con conseguenti deficit nella relativa gestibilità e nella possibilità di scalare industrialmente le soluzioni. Si sottolinea tale deficit in quanto la tendenza alla federazione dei Data Center delle PA, con conseguente interconnessione di basi dati e risorse elaborative, amplificherebbe gli effetti dell'eventuale violazione di un singolo CED. Inoltre, a livello organizzativo si segnala una disomogeneità nelle competenze del personale preposto alla conduzione dei sistemi informativi dei vari CED. Tale disomogeneità deriva dalle capacità di spesa delle singole PA, unitamente agli assetti organizzativi delle stesse che, in funzione della sensibilità dei rispettivi vertici, non sempre riconoscono l'informatica come fattore abilitante della missione e, conseguentemente, non investono in formazione e personale e del comparto ICT. Ancora a livello organizzativo, esistono gravi disarmonie tra le varie PA nella scelta di eventuali standard e processi per la conduzione dell'informatica in sicurezza.

Per quanto riguarda il piano in elaborazione da parte di AgID sulla razionalizzazione dei CED e l'armonizzazione dei processi di gestione della sicurezza, si nutrono per-

plessità sulle problematiche derivanti da una gestione unitaria degli stessi da parte di attori privati. Infatti, all'accentramento dei dati in un'unica infrastruttura corrisponde un maggior rischio di sicurezza qualora tali dati dovessero essere violati. L'aggregazione di dati eterogenei senza un'opportuna riflessione sulla natura degli stessi e sulle procedure di aggiornamento, inserimento e manutenzione rischia di essere un'attività fine a se stessa, se non addirittura dannosa. Occorre ponderare in modo sistematico quali infrastrutture accorpare e quali no. Inoltre, nel caso in cui si decidesse di investire nell'accorpamento di data center sarebbe auspicabile incrementare il ruolo delle amministrazioni nella gestione, manutenzione e potenziamento degli stessi in modo che non vengano date in outsourcing capacità strategiche per la sicurezza dei dati gestiti.

A tal riguardo si propongono le seguenti azioni:

- **lo sviluppo di un piano di evoluzione e consolidamento delle scelte strategiche, in linea con quanto in corso da parte di AgID;**
- **il lancio di un percorso di federazione dei CED che spinga i soggetti interessati a una razionalizzazione del parco dei servizi applicativi e all'adozione di standard di sicurezza comuni prima del consolidamento e, soprattutto, alla virtualizzazione dei CED stessi.**

Per quanto concerne le misure di sicurezza delle banche dati pubbliche e le modalità relative allo scambio dei dati personali tra le pubbliche amministrazioni, si segnala favorevolmente il provvedimento del 2 luglio 2015 del Garante per la protezione dei dati personali, secondo il quale le PA sono tenute a comunicare alla stessa Autorità Garante, entro 48 ore dalla conoscenza del fatto, tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali del cittadino. Si evidenzia inoltre come il bilanciamento tra privacy e security verrà ulteriormente potenziato dal nuovo ´Regolamento relativo alla protezione di persone fisiche con riguardo al trattamento dei dati personali` che entrerà in vigore nel Maggio 2018.

Cloud

La migrazione verso tecnologie cosiddette Cloud rappresenta certamente un passo verso la razionalizzazione delle risorse dei CED e verso soluzioni di Disaster Recovery/Business Continuity. Tuttavia condizione ineludibile per contenere un incremento

dell'esposizione al rischio in tale contesto, risiede nell'assicurare che tale migrazione in Cloud interessi un insieme di servizi e prodotti applicativi sufficientemente maturo, robusto e sicuro. Si rendono dunque necessarie, sotto formale impulso di indirizzo del legislatore, le seguenti azioni:

- **l'ammodernamento delle componenti applicative interessate che, spesso per difetto di costruzione o obsolescenza degli strumenti, lamentano debolezze intrinseche che, se pubblicate in Cloud, amplificherebbero il rischio di violazione;**
- **la definizione delle caratteristiche del "Cloud PA" in armonia con l'attuale architettura SPC (Sistema Pubblico di Connettività) onde consentire il recupero degli investimenti ed il consolidamento dei servizi già disponibili;**
- **la sistematizzazione di linee guida sui criteri di determinazione delle tipologie di dati da migrare su Cloud. Tale elemento, sebbene spesso non sufficientemente sottolineato da chi fornisce tali servizi, risulta di fondamentale importanza quando i dati da riversare su Cloud sono sensibili in termini sia di privacy, sia di sicurezza;**
- **la definizione di uno schema contrattuale standardizzato che indirizzi la completa e corretta attribuzione di responsabilità tra i fornitori e i fruitori dei servizi in Cloud;**
- **la promozione di soluzioni di Cloud e federazione tra Cloud in modalità 'sicura' tra pubbliche amministrazioni in modo da razionalizzare e efficientare le risorse informatiche a livello di sistema tra PP.AA. e non solo come soluzione verticale di ciascuna amministrazione.**

Open Source

Gli strumenti Open Source possono rivelarsi estremamente utili, portando, nel breve termine, a una sensibile riduzione dei costi. Giova tuttavia ricordare che l'open source è, prima che un modello commerciale, soprattutto un modello di sviluppo e per estendere al medio e lungo termine tale beneficio, occorre essere consapevoli che la gestione di strumenti open source (anche, ad esempio per servizi e non solo come strumenti lato client) richiede un investimento in termini di formazione e aggiornamento tecnologico a beneficio del personale dell'amministrazione allo scopo di ridurre i rischi derivanti da possibili attacchi intrinseci nella natura stessa di tali prodotti i cui codici sorgenti sono gestiti spesso in modalità "open o condivisa".

Le prospettive di risparmio delle soluzioni open source, peraltro, non sono sempre realistiche e, in caso di ricorso a tali prodotti disponibili in modalità cosiddetta community, la PA interessata dovrebbe dotarsi di personale specializzato interno, ovvero ricorrere a consulenze esterne il cui costo potrebbe rivelarsi comparabile con gli oneri di acquisto e gestione di prodotti proprietari. Tuttavia un investimento nella formazione del personale amministrativo permetterebbe di ridurre i significativi costi fissi ricorrenti ai quali tutte le amministrazioni sono sottoposte quando devono utilizzare strumenti commerciali di tipo closed source (ad esempio, le licenze software di prodotti per l'ufficio o di sistemi operativi).

A tal riguardo si propongono le seguenti misure:

- **una riflessione sui costi/benefici nel lungo termine della modalità open source e delle implicazioni a questa collegate in termini di formazione del personale;**
- **una riflessione alternativa sull'opportunità di richiedere alle maggiori aziende produttrici di software commerciale la disponibilità a realizzare per le PP.AA. versioni di sistemi operativi e applicativi per ufficio (wordprocessor, spreadsheet, ecc.) con costi di licensing contenuti e policy di aggiornamento centralizzate.**

Raccomandazioni dal mondo privato

L'approccio alla sicurezza è ancora prevalentemente orientato all'uso di misure di protezione perimetrale, che difficilmente possono fronteggiare una situazione in cui persone e strumenti sono sempre più in mobilità e le minacce vengono portate direttamente all'interno della rete aziendale. In uno scenario di questo tipo è fondamentale che le organizzazioni si focalizzino sulla protezione degli asset critici che, per una Pubblica Amministrazione, sono rappresentati dai dati dei cittadini considerati il bene più importante da proteggere.

La Cyber Security è, ormai, diventata una priorità a livello mondiale. Nonostante le notizie che giungono dal mondo portino sempre più alla ribalta la realtà di questa affermazione, i comportamenti delle organizzazioni e delle istituzioni sembrano minimizzare la magnitudo del problema e, di conseguenza, le azioni "correttive" tardano ad arrivare. Nel corso del 2014, mentre il numero complessivo degli attacchi informatici gravi di cui abbiamo avuto notizia è rimasto sostanzialmente invariato rispetto all'anno precedente, la gravità degli stessi è aumentata in modo significativo, sia in termini di quantità e di valore economico dei dati sottratti, sia in termini di ampiezza delle conseguenze nel caso di sabotaggi ed attacchi mirati su base internazionale. Questo perché sono aumentate, in parallelo, sia la sofisticazione e la determinazione degli attaccanti sia, di conseguenza, la severità dei danni subiti dalle vittime.

A seguire gli elementi correttivi che dovrebbero essere supportati dalle azioni governative:

- **necessità di aggiornare l'informatica esistente nella Pubblica Amministrazione superando inoltre l'obsolescenza informatica dell'infrastruttura esistente anche attraverso l'uso del Cloud Computing che mitiga rischi e diminuisce la superficie di attacco;**
- **messa in atto di procedure standard uguali a tutta la PA nel caso di violazioni alla sicurezza con la determinazione di chiare regole di ingaggio, di livelli di intervento e di responsabilità a capo di un numero ridotti di amministratori dei sistemi;**
- **messa a punto di soluzioni di gestione delle infrastrutture con particolare riferimento ai processi di aggiornamento dei sistemi (patch management) che risultano spesso incompleti e parziali e non coprono la grande varietà di software vulnerabile ad attacchi;**

- **istituzione di una strategia di sicurezza che copra gli aspetti di amministrazione, minimizzando il numero di utenti privilegiati e riducendo al minimo i privilegi amministrativi assegnati agli utenti, grazie all'aggiornamento delle piattaforme che oggi lo consentono;**
- **creazione di un piano di formazione per gli utenti che, spesso, attraverso i loro comportamenti minano la sicurezza aziendale - formazione estesa anche alla componente politica oltre a quella amministrativa;**
- **potenziamento delle capacità di individuazione tempestiva di un tentativo di intrusione. Gran parte delle misure attuali di monitoraggio sono finalizzate all'adempimento dei requisiti del Garante della Privacy sugli Amministratori di sistema, mentre raramente si utilizzano questi investimenti per migliorare le proprie capacità difensive. Diversi studi riportano come nella maggior parte degli incidenti di sicurezza, ci si renda conto di una compromissione mediamente 200 giorni dopo che l'attacco ha avuto inizio;**
- **realizzazione di processi strutturati di gestione degli incidenti di sicurezza, comprensivi della definizione di team dedicati alla sicurezza, di strumenti, di strategie di comunicazione interna ed esterna nonché di collaborazione con terze parti in grado di fornire supporto all'attività investigativa.**

Il principale ostacolo alla risoluzione dei problemi di obsolescenza viene identificato nella mancanza di copertura economica mentre la scarsa consapevolezza del management rispetto al livello di rischio si traduce nella lentezza nell'implementazione di contromisure e nella bassa priorità assegnata alla risoluzione dei problemi di sicurezza. Ma la sicurezza non è solo tecnologia, È innanzitutto un approccio culturale verso cui l'azienda deve essere proiettata. Le persone devono essere abituate a rispettare regole per garantire la sicurezza in azienda. La formazione deve avere un ruolo fondamentale nello sviluppare una cultura aziendale della sicurezza, sensibilizzare l'organizzazione e portarla a definire regole di comportamento a cui nessuno può sottrarsi. Tante minacce, infatti, possono arrivare anche dall'interno, attraverso scambi di e-mail, o navigando in Rete. L'approccio giusto alla sicurezza di un ente pubblico o privato non deve tralasciare né gli asset né le persone che vi lavorano. È essenziale una riforma della governance pubblica che preveda la presenza di un comitato pubblico-privato che affianchi il DIS e la Presidenza del Consiglio, leggasi unità di crisi, composto dalle principali aziende impegnate sulla cybersecurity operative 24/24 in casi di emergenza e regolare operatività (monitoraggio e controllo).

Conclusioni

La crescita esponenziale di attacchi informatici contro rilevanti comparti della pubblica amministrazione e il continuo aumento del livello di sofisticazione delle minacce rappresentano un fenomeno preoccupante che rappresenta un rischio concreto per il corretto ed efficiente funzionamento delle istituzioni. La prevenzione e il contrasto a tali minacce, nonché la risoluzione delle vulnerabilità presentate dagli apparati pubblici, sono conseguibili affiancando al miglioramento delle prestazioni delle strutture deputate all'area ICT, un impegno sul versante delle risorse umane. Spesso il dirigente pubblico è a conoscenza delle opportunità in termini di efficienza, efficacia e capacità di controllo offerte dalle ICT, ma non sempre è consapevole dei molteplici rischi legati alla crescente integrazione dei sistemi, delle reti, delle pratiche organizzative e dei comportamenti dei dipendenti pubblici e dei cittadini. La rivoluzione tecnologica impone, viceversa, la necessità stringente di ridefinire in termini nuovi le competenze, il ruolo e la cultura digitale del dirigente pubblico, nonché di ridisegnare – nel quadro di una visione unitaria e integrata – le molteplici strutture amministrative della pubblica amministrazione.

In questo senso si rende dunque indispensabile agire contemporaneamente in molteplici direzioni:

- **irrobustire i presidi tecnologici per la protezione delle reti e dei perimetri organizzativi della PA, anche attraverso una più ampia collaborazione tra i Computer Emergency Response Team (CERT, anche noti come CSIRT o Computer Security Incident Response Team) nazionali ed esteri;**
- **rafforzare il ruolo di istituzioni centrali preposte alla sicurezza informatica, quali ad esempio il CERT-PA , ampliando il loro ruolo anche con mansioni esecutive e di vera e propria consulenza nei confronti delle PA, con particolare riguardo a quelle più piccole che non possono avere la forza e le risorse per agire in autonomia;**
- **investire nella formazione e nella sensibilizzazione del capitale umano della PA;**
- **promuovere, da parte di AgiD, fra i dipendenti della PA iniziative che favoriscano la condivisione di informazioni utili a diversi scopi (sicurezza cibernetica negli uffici, garanzia degli appalti, formazione del personale, ecc.);**

- **prevedere lo sviluppo e la condivisione di percorsi, strumenti e materiali formativi di base da parte di AgID in modo da garantire, con un investimento centralizzato, un livello standard minimo di awareness sulla sicurezza di tutti i dipendenti della PA;**
- **istituire approfondite linee guida condivise per il buon utilizzo delle strumentazioni ICT da parte di tutti gli utenti. In questo senso va vista in modo molto favorevole l'adozione di regolamenti e standard di processo semplificati negli adempimenti meramente formali, ma non per questo meno efficaci, promulgati direttamente da questi enti (come le "Misure minime di sicurezza ICT" recentemente diffuse da AgID);**
- **stabilire una coerenza organizzativa, assegnando correttamente le responsabilità della gestione della sicurezza operativa;**
- **istituire un servizio assistenza di AgID a cui la PA possa rivolgersi in caso di problematiche riguardanti l'implementazione dei servizi digitali per favorire l'armonizzazione e l'interoperabilità delle strutture amministrative;**
- **promuovere e consolidare la partnership fra strutture pubbliche e private, nella consapevolezza che solo attraverso lo scambio di informazioni è possibile contribuire allo sviluppo di competenze nazionali;**
- **incentivare l'industria nazionale a sviluppare prodotti innovativi e all'avanguardia con specifiche personalizzazioni rivolte alla PA.**

La sicurezza informatica deve essere vista come un processo e non come uno stato che, una volta raggiunto, si mantiene unicamente attraverso la manutenzione dell'esistente. A tal proposito occorre pensare a vere e proprie campagne nazionali di penetration testing attraverso le quali si valutino in modo attivo le vulnerabilità delle infrastrutture della pubblica amministrazione e delle infrastrutture critiche di interesse nazionale e si propongano contromisure e soluzioni.

La rivoluzione digitale si pone come una sfida globale per tutti gli apparati statali che si affacciano al web 2.0. In questo senso, la pubblica amministrazione italiana è dunque chiamata a confrontarsi con le sfide che tale rivoluzione presenta, consapevole che nessun apparato, ufficio o singolo dipendente può essere lasciato in stato di vulnerabilità e che solo attraverso la messa in atto di concrete misure di sicurezza si può procedere verso una digitalizzazione del sistema amministrativo che sia efficace, efficiente e sicura.

Lista partecipanti

Partecipanti e enti di provenienza

Dott. Sergio ANTONICA - *Ivass*
Ing. Paolo BALDUCCI - *Ministero dello Sviluppo Economico*
Ing. Alessandro CALCHETTI - *Ministero dei Trasporti*
Ing. Clemente CARFORA - *Banca d'Italia*
Cons. Sarah CASTELLANI - *Ministero degli Esteri*
Dott. Mario CILLA - *Inps*
Dott.ssa Claudia COLAJACOMO - *Ministero dell'Economia e delle Finanze*
Dott. Roberto COPIA - *Ivass*
Claudia DI ANDREA - *Camera dei Deputati*
Dott.ssa Sabina DI GIULIOMARIA - *Banca d'Italia*
Dott.ssa Lidia DI MINCO - *Ministero della Salute*
Dott. Marco DOGLIA - *Ministero degli Esteri*
Ing. Mauro FIORONI - *Senato*
Dott. Carlo FOTI - *Ministero dell'Interno*
Dott. Valerio GENOVESE - *Presidenza del Consiglio*
Ing. Claudio GENTILI - *Consob*
Ing. Luigi IERNA - *Presidenza del Consiglio*
Dott. Roberto LATTANZI - *Garante della Privacy*
Ing. Fabio LAZZINI - *Sogei*
Dott.ssa Roberta LOTTI - *Ministero dell'Economia e delle Finanze*
Dott.ssa Vincenza PALOCCI - *Presidenza del Consiglio*
Col. Maurizio PENNAROLA - *Ministero della Difesa*
Dott. Gaetano REALE - *Dipartimento della Funzione Pubblica*
Dott. Gennaro SALESE - *Ministero della Giustizia*
Gen. D. Dino SCHIAVETTI - *Presidenza del Consiglio*
Ing. Giovanna TEBANO - *Consip*
Ing. Massimiliano ZAZZA - *Ministero dei Trasporti*

Sponsor

Ing. Sabino CAPORUSSO, *BV Tech*
Dott. Luigi MARTINO, *BV Tech*

Dott. Francesco BUTINI, *IDS*
Dott.ssa Sarah BARDELLI, *IDS*

Dott. Andrea BIRAGHI, *Leonardo*
Dott. Angeloluca BARBA, *Leonardo*
Dott. Felice DE PASCALE, *Leonardo*

Ing. Carlo MAUCELLI, *Microsoft*
Dott. Pier Luigi DAL PINO, *Microsoft*

Dott. Stefano GENOVESE, *Unipol*
Dott. Emilio DODARO, *Unipol*
Dott. Alberto RUSSO, *Unipol*

Organizzatori

Prof. Raffaele MARCHETTI, *LUISS (Direttore)*
Dott.ssa Roberta MULAS, *LUISS (Tutor)*

Prof. Marco MAYER, *SSSUP (Comitato Scientifico)*

Prof. Adriano SOI, *Università di Firenze (Comitato Scientifico)*

Redazione del testo a cura di Raffaele Marchetti, Roberta Mulas e Beatrice Valentina Ortalizio.

Con il patrocinio di

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

In collaborazione con

BV TECH

IDS
INGEGNERIA DEI SISTEMI

LEONARDO

Microsoft

Unipol
GRUPPO

LUISS School of Government
Via di Villa Emiliani, 14 - 00197 Rome (Italy)
www.sog.luiss.it - sog@luiss.it
+39 0685225065-52-53