Alla c.a. Dir. Caterina Graziani
Servizio Sicurezza, Infrastruttura e Architettura IT
SEDE

Oggetto: **MEPA - parere congruità su verifica di sicurezza su rete wi-fi intranet.**

Il presente documento rappresenta la relazione tecnico-illustrativa e valutazione comparativa redatta dal RUP ai sensi dell'art. 23 comma15 del D.Lgs. 50/2016 e ss.mm.ii.

Il Comune di Firenze dispone di un'estesa rete metropolitana realizzata tramite apparati e tecnologie di connettività basate su collegamenti wired (cablati) e Wi-Fi (senza fili). Questa infrastruttura è gestita interamente dalla Direzione Sistemi Informativi ed è in continua crescita per arrivare a coprire capillarmente tutte le sedi e gli uffici con un adeguato livello di connettività. Il Comune di Firenze, per incrementare la sicurezza informatica di accesso alla rete intranet, ha attivato una soluzione open source su tecnologia NAC (Network Access Control) per l'abilitazione della rete ai solo dispositivi autorizzati, in corso di sperimentazione in alcune sedi. All'interno del progetto di dispiegamento del NAC, oltre alla rete cablata, è prevista l'attivazione anche per la rete intranet via Wi-Fi con accesso tramite protocollo di autenticazione "802.1x e *MAC (Media Access Control) authentication*". Allo stato dell'arte la parte Wi-Fi intranet è stata attivata solo presso la sede della Direzione Sistemi Informativi e i test iniziali hanno dimostrato, al momento, stabilità e sufficiente robustezza della soluzione.

La continua espansione delle tecnologie informatiche come strumenti di lavoro, la diffusione dei servizi cloud e le diverse modalità di interconnessione hanno portato ad una crescita dell'area di esposizione agli attacchi informatici e ad una maggiore vulnerabilità dell'intero spazio cibernetico. La Cybersecurity (sicurezza informatica) diventa un reale rischio per ogni organizzazione ed è fondamentale cercare di intraprendere azioni preventive e proattive per assicurare la continuità dei sistemi in caso di attacchi informatici e per irrobustire le soluzioni e le configurazioni già in essere. Pertanto, la tematica di condurre delle sessioni di indagine, di testing, di ricerca e di individuazione di eventuali vulnerabilità (*vulnerability assessment*) rappresenta un elemento critico nel processo di analisi e riduzione rischi, aspetti su cui un'organizzazione deve porre sempre più attenzione.

Dato che la sicurezza informatica è un punto imprescindibile per il corretto funzionamento e l'erogazione dei servizi, è stato deciso di effettuare dei test di "*ethical hacking*" per valutare la sicurezza della rete Wi-Fi intranet prima di procedere con l'eventuale attivazione in altre sedi. A seguito delle attività condotte saranno prodotte due relazioni: una di sintesi con una panoramica sulla situazione rilevata e le indicazioni sui macro-passi principali da portare avanti per migliorare i livelli di sicurezza e l'altra con i dettagli tecnico-informatici contenenti le analisi, le problematiche riscontrate, le azioni di contenimento proposte, le azioni di bonifica e correzione (*remediation*) di quanto individuato. Si richiede che tra le parti sia firmato un accordo preventivo di *Non-Disclosure Agreement* (NDA) per tutelare l'Ente sulle vulnerabilità rilevate.

Attualmente le attività di configurazione e di supporto sulla soluzione NAC e del wi-fi sono assicurate dall'aziena UniRel s.r.l., oltre che da personale interno della DSI, quindi è indispensabile

Via Reginaldo Giuliani 250 * 50141 Firenze * tel. 055 3283807 * fax 055 3283823
e-mail: direzione.sistemiinformativi@comune.fi.it

che le verifiche sopra indicate siano condotte da un soggetto terzo, totalmente estraneo ai tecnici che attualmente gestiscono la soluzione tecnologica oggetto dell'attività di *vulnerability assessment*.

Ad oggi non risultano convenzioni o accordi quadro CONSIP attivi per coprire il servizio cercato, anche se nei prossimi mesi dovrebbe venirne aggiudicato qualcuno, però con importi di accesso più alti (Importo Minimo d'Ordine - IMO). Pertanto, pur nella complessità che caratterizza un servizio di questo tipo, spesso in dipendenza della rete aziendale su cui eseguirlo, è stata condotta una ricerca sul Mercato Elettronico per la Pubblica Amministrazione (MEPA) per identificare un'offerta che rispondesse a tutti i vincoli indicati e presentasse caratteristiche possibilmente standard o di mercato, questo anche nell'ottica futura di rieseguire i controlli ricorrendo però a fornitori diversi per quanto già precisato. Alla fine è stato possibile individuare alcune offerte e dalla loro comparazione si riscontra un livello sufficiente di standardizzazione e stessa tipologia di attività previste nell'eseguire un *vulnerability assessment*, quindi, almeno per l'importo presunto per singola rete Wi-Fi, riconducibili a conduzioni definite dal mercato. In questo caso, pertanto, è stato valutato di non ricorrere ad una valutazione tecnico-comparativa su funzioni e qualità, ma viene applicato il criterio del minor prezzo (art. 95 comma 4 lettera 'b' del D.Lgs. 50/2016 e ss.mm.ii.). Tenuto conto dell'importo presunto e delle caratteristiche standard della fornitura, si sceglie di procedere ad un affidamento diretto ai sensi dell'art. 1 comma 2 lett. a) del D.L. 76/2020 tramite lo strumento tecnico dell'Ordine Diretto (OD) su MEPA.

Come premesso, sono presenti più offerte che possono soddisfare le necessità elencate e, valutando il costo minore indicato sul portale, è stato scelto l'articolo/servizio pubblicato dalla ditta Axians Brand id S.p.A. che presenta le caratteristiche cercate.
L'articolo è identificato dal seguente codice:
codice "VUL ASS", importo unitario € 5.292,00 + IVA

La soluzione individuata è economicamente vantaggiosa, compatibile con le necessità dell'Ente e tecnologicamente rispondente ai requisiti individuati per condurre il *vulnerability assessment* sul servizio Wi-Fi, pertanto si può procedere con il relativo ordine MEPA.
Il costo presunto della fornitura di **€ 5.292,00 + IVA** è congruo.

Il responsabile della
P.O. Data center, sistemi e cloud
(interim) P.O. Reti, Multimedialità e IoT

Ing. Luca Bertelli

BERTELLI
LUCA
09.03.2022
11:12:08
GMT+00:00

Via Reginaldo Giuliani 250 * 50141 Firenze * tel. 055 3283807 * fax 055 3283823
e-mail: direzione.sistemiinformativi@comune.fi.it