Area Risorse - Servizio Appalti e contratti

U.O.C. Acquisti Appalti Contratti - Via San Pietro Martire, 3 - 42121 Reggio nell'Emilia (RE)
tel. 0522.456889 - 456121 - fax. 0522.456037 - http://www.comune.re.it/gare
Partita I.V.A. e C.F.: 00145920351
PEC: uocappalticontratti@pec.municipio.re.it – E-mail: garesenzacarta@comune.re.it

Prot. ….(n. di protocollo assegnato automaticamente dalla piattaforma di gara)

Pubblicazione a mezzo piattaforma di gara Sater di Intercent-ER

Reggio nell'Emilia, 21 Maggio 2021

PROCEDURA APERTA TRAMITE SATER DI INTERCENT-ER PER L'AFFIDAMENTO DISGIUNTO DI SERVIZI ASSICURATIVI OCCORRENTI AL COMUNE DI REGGIO EMILIA - PERIODO DALLE ORE 24 DEL 30/06/2021 ALLE ORE 24 DEL 31/12/2023 CPV 66510000-8:

- **LOTTO 1 POLIZZA INCENDIO BENI COMUNI, BENI DI PREGIO, FURTO: CUI S00145920351202000033 - CIG 8737792E0D;**
- **LOTTO 2 POLIZZA INFORTUNI CUMULATIVA: CUI S00145920351202000037 - CIG 873785520E ;**
- **LOTTO 3 POLIZZA RC PATRIMONIALE: CUI S00145920351202000035 - CIG 8737887C73;**
- **LOTTO 4 POLIZZA KASKO: CUI S00145920351202000031 - CIG 87379207B0 ;**
- **LOTTO 5 POLIZZA CYBER RISCHI INFORMATICI: CUI S00145920351202000038 - CIG 8738081C8B.**

Alla Stazione Appaltante, è pervenuto il seguente quesito, che si riporta a seguire, unitamente alla relativa risposta:

QUESITO N. 1

LOTTO 5 POLIZZA CYBER RISCHI INFORMATICI

Buongiorno,
con la presente, siamo a richiedere la compilazione dei seguenti quesiti in merito al lotto Cyber Risk:

1.1. Per quanto riguarda le attività messe in campo dal Richiedente per mitigare il phishing, selezionare tutte le risposte pertinenti

- *Il Richiedente eroga, almeno una volta all'anno, ai dipendenti formazione sulla "consapevolezza della sicurezza informatica"*
- *Il Richiedente, almeno una volta all'anno, utilizza attacchi di phishing simulati per testare la consapevolezza della sicurezza informatica dei dipendenti*
- *Qualora il Richiedente conduca attacchi di phishing simulati, la percentuale di successo nell'ultimo test è stata inferiore al 15% (meno del 15% dei dipendenti è stato "indotto in errore" con successo)*

- *Il Richiedente "contrassegna", o comunque evidenzia in altro modo, tutte le e-mail provenienti dall'esterno dell'organizzazione.*
- *Il Richiedente ha un processo per segnalare e-mail sospette a un team di sicurezza interno che ha il compito di indagare*
- *Nessuno dei precedenti.*
- *Commento aggiuntivo sugli sforzi per mitigare il phishing:*

1.2 Il Richiedente dispone di un processo documentato per rispondere alle campagne di phishing (mirate specificamente al Richiedente o meno)?

- *Si*
- *No*

Se "Sì", descrivere i passaggi principali della risposta

1.3 Per quanto riguarda le attività/presidi di sicurezza adottati dal Richiedente per bloccare siti web e / o email potenzialmente dannose, selezionare tutte le risposte pertinenti:

- *Il Richiedente utilizza una soluzione di filtraggio della posta elettronica che blocca allegati dannosi noti e tipi di file sospetti, inclusi gli eseguibili*
- *Il Richiedente utilizza una soluzione di filtro della posta elettronica che blocca i messaggi sospetti in base al contenuto o agli attributi del mittente*
- *Il Richiedente utilizza una soluzione di filtraggio web che impedisce ai dipendenti di visitare pagine web dannose o sospette note*
- *Il Richiedente utilizza blocchi verso domini non categorizzati e/o di nuova registrazione utilizzando proxy Web o filtri DNS*
- *Il Richiedente utilizza una soluzione di filtro web che blocca i download noti come dannosi o sospetti, inclusi gli eseguibili*
- *La soluzione di filtraggio della posta elettronica del Richiedente ha la capacità di eseguire allegati sospetti in una sandbox*
- *Le funzionalità di filtro web del Richiedente sono efficaci su tutte le risorse aziendali, anche se la risorsa aziendale non si trova su una rete aziendale (ad esempio, le risorse sono configurate per utilizzare filtri web basati su cloud o richiedono una connessione VPN per navigare in Internet).*
- *Nessuno dei precedenti*
- *Commenti aggiuntivi attività/presidi di sicurezza adottati dal Richiedente per bloccare siti Web e / o e-mail dannose*

1.4 Per quanto riguarda l'autenticazione per i dipendenti che accedono da remoto alla rete aziendale e a qualsiasi servizio basato su cloud in cui possono risiedere dati sensibili (incluso l'accesso alla VPN, la posta elettronica e i CRM basati su cloud; definiti come "accesso remoto alle risorse aziendali), selezionare la descrizione che meglio riflette la postura del Richiedente [nota: nel presente documento, "autenticazione a più fattori" – MFA - significa un'autenticazione che utilizzi almeno due diversi tipi di possibili fattori di autenticazione (qualcosa che sai, qualcosa hai e qualcosa che sei); il Richiedente può fornire ulteriori spiegazioni di seguito]

- *L'accesso remoto alle risorse aziendali richiede un nome utente e una password validi (autenticazione a fattore singolo)*
- *L'autenticazione a più fattori è attiva per alcuni tipi di accesso remoto alle risorse aziendali, ma non tutti*
- *L'autenticazione a più fattori è richiesta dalla politica per tutti gli accessi remoti alle risorse aziendali; tutte le eccezioni alla politica sono documentate*

- *Il Richiedente non fornisce l'accesso remoto ai dipendenti*
- *Commento aggiuntivo sull'autenticazione per i dipendenti:*

1.5 "Per quanto riguarda l'autenticazione per appaltatori e fornitori indipendenti che accedono in remoto alla rete aziendale e a qualsiasi servizio basato su cloud in cui i dati sensibili possono risiedere (compreso

- *l'accesso VPN, e-mail e CRM basati su cloud; tutti insieme definiti come ""accesso remoto alle risorse aziendali""), selezionare la descrizione che meglio riflette la posizione del Richiedente: (Il Richiedente può fornire ulteriori spiegazioni di seguito)"*
- *L'accesso remoto alle risorse aziendali richiede un nome utente e una password validi (autenticazione a fattore singolo)*
- *L'autenticazione a più fattori è attiva per alcuni tipi di accesso remoto alle risorse aziendali, ma non tutti.*
- *L'autenticazione a più fattori è richiesta dalla politica per tutti gli accessi remoti alle risorse aziendali; tutte le eccezioni alla politica sono documentate.*
- *Il Richiedente non fornisce l'accesso remoto a contraenti / fornitori indipendenti*
- *Commento aggiuntivo sull'autenticazione per appaltatori / fornitori indipendenti:*

1.6 "L'implementazione dell'autenticazione a più fattori del Richiedente soddisfa anche il criterio secondo cui la compromissione di un singolo dispositivo comprometterà solo un singolo autenticatore?
(Ad esempio: se l'autenticazione richiede una password (conoscenza) e un token (possesso), di per se stesso il criterio di cui sopra non sarebbe soddisfatto là dove il token per dimostrare il possesso sia mantenuto sul medesimo dispositivo che conserva anche la password, esponendoli entrambi i fattori se il dispositivo fosse compromesso)"

- *Non applicabile (il Richiedente non utilizza l'autenticazione a più fattori)*
- *No; L'implementazione multifattoriale del Richiedente non soddisfa i criteri di cui sopra.*
- *Sì; l'implementazione multifattoriale del Richiedente soddisfa i criteri di cui sopra.*
- *Commento aggiuntivo sull'implementazione dell'autenticazione a più fattori:*

1.7 Per quanto riguarda la sicurezza degli endpoint e delle workstation (desktop e laptop) del Richiedente, selezionare tutte le risposte pertinenti:

- *La politica del Richiedente è che tutte le workstation siano dotate di antivirus con funzionalità euristiche (non basate solo su firma)*
- *Il Richiedente utilizza strumenti di sicurezza degli endpoint con funzionalità di rilevamento del comportamento e mitigazione degli exploit.*
- *Il Richiedente dispone di un gruppo interno che monitora l'output degli strumenti di sicurezza degli endpoint e indaga su eventuali anomalie.*
- *Nessuno dei precedenti.*
- *Commento aggiuntivo sulle funzionalità di sicurezza degli endpoint:*

1.8 Per quanto riguarda il monitoraggio delle log (segnalazioni) degli strumenti di sicurezza, selezionare la descrizione che meglio riflette la capacità di gestione del Richiedente:

- *Il Richiedente non dispone di personale dedicato al monitoraggio delle operazioni di sicurezza (un "Centro operativo di sicurezza – c.d. SOC: Security Operations Center ")*

- *Il Richiedente ha un Security Operations Center, ma non è attivo 24 ore su 24, 7 giorni su 7 (può essere interno o esterno)*
- *Il Richiedente ha un monitoraggio 24 ore su 24, 7 giorni su 7 delle operazioni di sicurezza da parte di una terza parte (es. un Fornitore di Servizi di Sicurezza Gestiti c.d. Managed Security Services Provider)*
- *Il Richiedente ha un monitoraggio interno 24 ore su 24, 7 giorni su 7 delle operazioni di sicurezza*
- *Commento aggiuntivo sul monitoraggio della sicurezza:*

1.9 Qual è stato il tempo medio necessario al Richiedente per valutare e contenere gli incidenti di sicurezza delle workstation dall'inizio dell'anno?

- *Il Richiedente non tiene traccia di questa metrica / Non lo so*
- *meno di 30 minuti*
- *30 minuti-2 ore*
- *2-8 ore*
- *Più di 8 ore*
- *Commento aggiuntivo sul tempo medio per rimediare:*

1.10 Per quanto riguarda i controlli di accesso per la postazione di lavoro di ogni utente, selezionare la descrizione che meglio riflette la postura del Richiedente (Il Richiedente può fornire ulteriori spiegazioni di seguito):

- *Nessun dipendente è nel gruppo degli amministratori o ha accesso come amministratore locale alla propria workstation*
- *La politica del Richiedente prevede che i dipendenti per impostazione predefinita non siano nel gruppo degli amministratori e non abbiano accesso amministrativo locale; tutte le eccezioni alla politica sono documentate*
- *Alcuni dipendenti del Richiedente fanno parte del gruppo degli amministratori o sono amministratori locali*
- *Non lo so*
- *Commento aggiuntivo sui controlli di accesso per le workstation:*

1.11 Per quanto riguarda la protezione delle credenziali privilegiate, selezionare tutto ciò che si applica rispetto alla postura del Richiedente

- *Gli amministratori di sistema del Richiedente dispongono di una credenziale unica e privilegiata per le attività amministrative (separata dalle credenziali utente per l'accesso quotidiano, e-mail, ecc.)*
- *Gli account privilegiati (inclusi gli amministratori di dominio) richiedono l'autenticazione a più fattori*
- *Gli account privilegiati sono conservati in una cassaforte per password che richiede all'utente di "estrarre" le credenziali (che vengono ruotate in seguito)*
- *È disponibile un registro di tutti gli utilizzi degli account privilegiati per almeno gli ultimi trenta giorni*
- *Le workstation ad accesso privilegiato (workstation che non hanno accesso a Internet o alla posta elettronica) vengono utilizzate per l'amministrazione di sistemi critici (inclusi server di autenticazione /Controller di dominio)*
- *Nessuno dei precedenti*
- *Commento aggiuntivo sulla protezione delle credenziali privilegiate:*

1.12 Fornire dettagli sull'utilizzo da parte del Richiedente di Microsoft Active Directory (in tutti i domini / foreste):

- *Il Richiedente non utilizza Microsoft Active Directory (indicare a destra)*
- *Numero di account utente nel gruppo del Dominio Amministratori (inclusi gli account di servizio, se presenti, in questo totale)*
- *"Numero di account di servizio nel gruppo del Dominio Amministratori: (”" account di servizio "" indica un account utente creato appositamente per un'applicazione*
- *o un servizio per interagire con altri computer*
- *appartenenti a un dominio):"*
- *Commento aggiuntivi sul numero degli amministratori di dominio*

1.13 "Quanti utenti hanno account con privilegi permanenti per gli endpoint (server e workstation)?
(Ai fini di questa domanda, ""account con privilegi"" indica i diritti per configurare, gestire e supportare in altro modo questi endpoint; gli utenti che devono ""effettuare il check-out"" delle credenziali non dovrebbero essere inclusi. Il Richiedente può fornire ulteriori spiegazioni di seguito)"

- *Inserisci un numero intero*
- *Commento aggiuntivo sul numero di accountcon privilegi*

1.14 Per quanto riguarda la sicurezza dei sistemi esposti verso l'esterno, selezionare tutto ciò che si applica alla postura del Richiedente

- *Il Richiedente esegue un test di penetrazione almeno una volta all'anno per valutare la sicurezza dei suoi sistemi rivolti verso l'esterno*
- *Il Richiedente ha un Web Application Firewall (WAF) davanti a tutte le applicazioni rivolte all'esterno ed è in modalità di blocco*
- *Il Richiedente utilizza un servizio esterno per monitorare la sua superficie di attacco (sistemi esterni / rivolti a Internet)*
- *Nessuno dei precedenti*

1.15 Qual è il tempo target del Richiedente per distribuire le patch "critiche" intendendosi quelle di massima priorità (come determinata dagli standard del Richiedente per la distribuzione delle patch)?

- *Non esiste una politica definita per la distribuzione delle patch.*
- *Entro 24 ore*
- *24-72 ore*
- *3-7 giorni*
- *> 7 giorni*
- *Commento aggiuntivo sui tempi target per l'applicazione delle patch*

1.16 Qual è stata il livello di conformità da inizio anno del Richiedente ai propri standard per la distribuzione di patch critiche? (Il Richiedente può fornire ulteriori spiegazioni di seguito)

- *Il Richiedente non tiene traccia di questa metrica / Non lo so*
- *>95%*
- *90-95%*
- *80-90%*
- *<80%*
- *Commento aggiuntivo sulla conformità delle patch:*

1.17 Per quanto riguarda le capacità di monitoraggio della rete del Richiedente, selezionare tutte le risposte pertinenti:

- *Il Richiedente utilizza uno strumento SIEM (Security Information and Event Monitoring) per correlare l'output di più strumenti di sicurezza*
- *Il Richiedente monitora il traffico di rete per trasferimenti di dati anomali e potenzialmente sospetti*
- *Il Richiedente monitora i problemi di prestazioni e capacità di archiviazione (come utilizzo elevato della memoria o del processore o assenza di spazio libero su disco).*
- *Il Richiedente dispone di strumenti per monitorare la perdita di dati (DLP) e sono in modalità di blocco.*
- *Nessuno dei precedenti*
- *Commento aggiuntivo sul monitoraggio della rete:*

1.18 "Relativamente alla limitazione dei movimenti laterale, selezionare tutto ciò che si applica alla postura del Richiedente
(Il Richiedente può fornire ulteriori spiegazioni di seguito):"

- *Il Richiedente ha segmentato la rete in base all'area geografica (e.g.: il traffico tra uffici in luoghi diversi è negato a meno che non sia richiesto per supportare uno specifico requisito aziendale)*
- *Il Richiedente ha segmentato la rete in base alla funzione aziendale (ad esempio il traffico tra asset che supportano funzioni diverse, ad esempio HR e Finance, è negato a meno che non sia richiesto per supportare uno specifico requisito aziendale*
- *Il Richiedente ha implementato regole del firewall host che impediscono l'uso di Remote Desktop Protocol - RDP per accedere alle workstation*
- *Il Richiedente ha configurato tutti gli account di servizio per negare gli accessi interattivi*
- *Nessuno dei precedenti*
- *Commento aggiuntivo sulla segmentazione:*

1.19 Immettere la data dell'ultima esercitazione su ransomware da parte del Richiedente ovvero selezionare l'apposita casella se non ne è stata eseguita nessuna esercitazione

- *Data:*
- *Non è stata condotta alcuna esercitazione su ransomware*

1.20 Il Richiedente dispone di un piano documentato per rispondere al ransomware di un fornitore / fornitore di terze parti o cliente? In caso affermativo, indicare i passaggi principali

- *No*
- *Sì*
- *Fasi principali della risposta al ransomware di terze parti:*

1.21 "Per quanto riguarda la verifica dell'efficacia dei controlli di sicurezza, selezionare tutto ciò che si applica al Richiedente
(Il Richiedente può fornire ulteriori spiegazioni di seguito)"

- *Il Richiedente utilizza software BAS (Breach and Attack Simulation) per verificare l'efficacia dei controlli di sicurezza*
- *Il Richiedente dispone di un "red team" interno che verifica i controlli di sicurezza e la risposta*

- *Nell'ultimo anno Il Richiedente ha incaricato un fornitore esterno di simulare gli attori delle minacce e testare i controlli di sicurezza*
- *Nessuno dei precedenti*
- *Commento aggiuntivo sulla verifica dei controlli:*

1.22 Per quanto riguarda le funzionalità di ripristino di emergenza, selezionare tutto ciò che si applica al Richiedente:

- *Esiste un processo per la creazione di backup, ma non è documentato e/o ad hoc*
- *Il Richiedente dispone di una politica di ripristino di emergenza documentata, inclusi standard per i backup basati sulla criticità delle informazioni*
- *Almeno due volte all'anno, il Richiedente verifica la propria capacità di ripristinare tempestivamente diversi sistemi e dati critici dai propri backup*
- *Nessuno dei precedenti*

1.23 Qual è l'RTO (Recovery Time Objective) del Richiedente per i sistemi critici?

- *Il Richiedente non ha un RTO / Non lo sa*
- *< 4 ore*
- *4-24 ore*
- *1 to 2 giorni*
- *2-7 giorni*

1.24 Per quanto riguarda le capacità di backup, selezionare tutto ciò che si applica al Richiedente:

- *La strategia di backup del Richiedente include backup offline (possono essere archiviati in sede)*
- *La strategia di backup del Richiedente include backup offline archiviati fuori sede*
- *È possibile accedere ai backup del Richiedente solo tramite un meccanismo di autenticazione esterno alla nostra Active Directory aziendale*
- *Commento aggiuntivo sulle funzionalità di backup:*

1.25 Il Richiedente dispone di una politica in base alla quale tutti i dispositivi portatili utilizzano la crittografia completa del disco?

- *Sì*
- *No*
- *Commento aggiuntivo:*

RISPOSTA A QUESITO N. 1

1.1
Il Richiedente ha un processo per segnalare e-mail sospette a un team di sicurezza interno che ha il compito di indagare
Commento aggiuntivo sugli sforzi per mitigare il phishing: Formazione privacy obbligatoria con modulo formativo specifico sul phishing e sulla sicurezza informatica a protezione dei dati personali tarato sulla realtà dell'Ente in corso di distribuzione a tutti i dipendenti. Intenzione, compatibilmente con le risorse economiche, di attivare piattaforma di formazione specifica con possibilita' di attacchi simulati .

1.2

Si
Vedi par “7.5 Suggerimenti per la prevenzione da malware” del Disciplinare per utenti dei sistemi informativi (sezione Privacy della intranet)

1.3
Il Richiedente utilizza una soluzione di filtraggio della posta elettronica che blocca allegati dannosi noti e tipi di file sospetti, inclusi gli eseguibili
Il Richiedente utilizza una soluzione di filtro della posta elettronica che blocca i messaggi sospetti in base al contenuto o agli attributi del mittente
Il Richiedente utilizza una soluzione di filtraggio web che impedisce ai dipendenti di visitare pagine web dannose o sospette note
Il Richiedente utilizza una soluzione di filtro web che blocca i download noti come dannosi o sospetti, inclusi gli eseguibili
La soluzione di filtraggio della posta elettronica del Richiedente ha la capacità di eseguire allegati sospetti in una sandbox

1.4
L'accesso remoto alle risorse aziendali richiede un nome utente e una password validi (autenticazione a fattore singolo)
Commento aggiuntivo sull'autenticazione per i dipendenti: E' stata implementato un sistema di autenticazione a più fattori per l'accesso remoto alle risorse aziendali. Tale sistema è già stato configurato in test per le applicazioni più critiche ed è in corso di messa in produzione.
Inoltre sono stati adeguati i requisiti dei modelli gara per richiederlo obbligatoriamente nelle future acquisizioni.

1.5
L'accesso remoto alle risorse aziendali richiede un nome utente e una password validi (autenticazione a fattore singolo)
Commento aggiuntivo sull'autenticazione per appaltatori / fornitori indipendenti: accedono tramite utente e certificato alla vpn e tramite utente e password alla singola applicazione

1.6
Non applicabile (il Richiedente non utilizza l'autenticazione a più fattori)
Commento aggiuntivo sull'implementazione dell'autenticazione a più fattori: in corso di attivazione l'autenticazione a più fattori per alcuni tipi di accesso remoto alle risorse aziendali. Quando attivo soddisfera’ il criterio al punto 6

1.7
La politica del Richiedente è che tutte le workstation siano dotate di antivirus con funzionalità euristiche (non basate solo su firma).
Il Richiedente utilizza strumenti di sicurezza degli endpoint con funzionalità di rilevamento del comportamento e mitigazione degli exploit.
Il Richiedente dispone di un gruppo interno che monitora l'output degli strumenti di sicurezza degli endpoint e indaga su eventuali anomalie.

1.8
Il Richiedente ha un monitoraggio 24 ore su 24, 7 giorni su 7 delle operazioni di sicurezza da parte di una terza parte (es. un Fornitore di Servizi di Sicurezza Gestiti c.d. Managed Security Services Provider)

1.9
2-8 ore

1.10
La politica del Richiedente prevede che i dipendenti per impostazione predefinita non siano nel gruppo degli amministratori e non abbiano accesso amministrativo locale; tutte le eccezioni alla politica sono documentate

1.11
Gli amministratori di sistema del Richiedente dispongono di una credenziale unica e privilegiata per le attività amministrative (separata dalle credenziali utente per l'accesso quotidiano, e-mail, ecc.)

1.12
"Numero di account di servizio nel gruppo del Dominio Amministratori: ("" account di servizio "" indica un account utente creato appositamente per un'applicazione o un servizio per interagire con altri computer appartenenti a un dominio):" 11

1.13
11 + 14 utenti di sw house con admin server

1.14
Il Richiedente utilizza un servizio esterno per monitorare la sua superficie di attacco (sistemi esterni / rivolti a Internet)

1.15
3-7 giorni

1.16
Il Richiedente non tiene traccia di questa metrica / Non lo so

1.17
Il Richiedente monitora il traffico di rete per trasferimenti di dati anomali e potenzialmente sospetti.
Il Richiedente monitora i problemi di prestazioni e capacità di archiviazione (come utilizzo elevato della memoria o del processore o assenza di spazio libero su disco).

1.18
Nessuno dei precedenti
Commento aggiuntivo sulla segmentazione: l’RDP sui server e’ regolato dal firewall e in generale rdp su server e workstation utilizzabile solo da account abilitati

1.19
Non è stata condotta alcuna esercitazione su ransomware

1.20
No

1.21
Nessuno dei precedenti

1.22
Il Richiedente dispone di una politica di ripristino di emergenza documentata, inclusi standard per i backup basati sulla criticità delle informazioni

1.23
2-7 giorni

1.24
La strategia di backup del Richiedente include backup offline archiviati fuori sede
Commento aggiuntivo sulle funzionalità di backup: il backup offline e' fatto tramite clone su sistemi in altra sede rispetto al DC dell'ente

1.25
No
Commento aggiuntivo: L'Ente fornisce indicazioni a tutti i dipendenti per la cifratura dei file sui dispositivi portatili, memorie esterne, chiavette usb e per l'invio di file tramite mail all'esterno dell'Ente, sia attraverso la formazione privacy obbligatoria, sia tramite le schede pubblicate nella intranet aziendale che contengono una modulistica ad hoc.

Il Dirigente del Servizio Appalti e Contratti
(F.to dott. Alberto Prampolini)