Informazioni Generali

1. **Budget IT (budget per hardware, software, personale e outsourcing. Calcolato su base annua: costi di investimento in asset IT (CapEx) + costi operativi (OpEx), esclusi ammortamenti)** 195k €
2. **Budget IT Security (budget per attività di Security Operations, attività di Security Awareness, Penetration Tests / Vulnerability Assessment, ecc.):** non calcolato
3. **Certificazioni:**
4. **Quali tipi di incidenti di sicurezza ha affrontato l'azienda negli ultimi 12 mesi? Ulteriori dettagli sulle categorie possono essere trovati nella ENISA Threat Taxonomy:** Nessun incidente

Organizzazione e Governance della Sicurezza IT

5. **L'azienda ha un "Chief Information Security Officer" (CISO) designato o un team che riporta regolarmente alla direzione?** è stato nominato il Referente per la Cybersicurezza
6. **L'azienda ha stabilito una politica di sicurezza delle informazioni?** Si
7. **È definito e applicato un programma di sensibilizzazione alla sicurezza delle informazioni che garantisce che tutto il personale e i collaboratori ricevano una formazione adeguata e aggiornamenti regolari sulle politiche e procedure organizzative, rilevanti per la loro funzione lavorativa?** Si
8. **L'azienda ha un piano strategico per la sicurezza informatica?** Si

Controllo degli Accessi

9. **È definita e pubblicata una politica di controllo degli accessi logici?** Definita si, pubblicata no
10. **È implementato un processo formale di gestione degli account utente e dei profili (ad esempio, richiesta utente, creazione, eliminazione, assegnazione del profilo di accesso) per l'accesso ai sistemi e ai dati?** è in fase di implementazione
11. **Viene periodicamente effettuata la revisione dei diritti di accesso e dei profili degli utenti e degli amministratori, al fine di identificare possibili conflitti nella Separazione dei Compiti (SoD)?** Si
12. **È definita una politica che stabilisce le regole essenziali per la complessità e la conservazione delle password?** Si
13. **Come gestisce l'azienda i rischi introdotti dall'uso di dispositivi mobili?** hw encription disk
14. **Come protegge l'azienda l'accesso remoto ai sistemi/reti IT interni?** VPN
15. **È definito un perimetro di sicurezza e implementati controlli di accesso fisico per proteggere le aree che contengono informazioni critiche e strutture di elaborazione delle informazioni? Ad esempio, registri di accesso/uscita e CCTV nei Data Center:** Data Center Segregato/Chiavi solo al RPC
16. **Sono definite e implementate procedure di smaltimento o riutilizzo sicuro delle apparecchiature? Ad esempio, sanificazione dei supporti di memorizzazione, ecc.** I rifiuti RAEE vengono smaltiti con azienda apposita/ non sono presenti dati sui PC, solo in cloud

Gestione del Rischio

17. **Sono definite procedure di gestione del rischio?** Si
18. **È definito e implementato un processo di valutazione del rischio IT?** Si

19. **È definito, aggiornato e monitorato un piano di mitigazione?** Si
20. **L'azienda tiene un inventario di tutti gli asset software e hardware?** Si
21. **L'azienda esternalizza uno o più dei seguenti servizi?** Si
22. **L'azienda esegue valutazioni del rischio prima di condurre affari con aziende di software esterne o fornitori di servizi?** Si
23. **Quali tipi di dati sensibili mantiene/elabora la tua azienda?**
24. **Come gestisce l'azienda la classificazione delle informazioni?**

Continuità Operativa e Gestione degli Incidenti

25. **L'azienda ha definito l'Obiettivo del Punto di Recupero (RPO) dei sistemi/servizi IT, in conformità con la strategia di Disaster Recovery?** sistema in aggiornamento
26. **Fornire RPO:** <6 ore
27. **Come gestisce l'azienda i backup?** I backup vengono eseguiti quotidianamente
28. **Ogni quanto tempo l'Azienda testa i backup?** 3 Mesi
29. **Con quale frequenza l'azienda esegue i backup dei dati critici per il business?** Quotidianamente
30. **Gli asset e i sistemi informativi sono monitorati per identificare eventi di sicurezza informatica e verificare l'efficacia delle misure protettive?** Si, con MDR
31. **L'azienda ha un piano di risposta agli incidenti per violazioni dei dati, intrusioni di rete o infezioni da malware?** Si, in revisione costante

Sicurezza delle Minacce, Vulnerabilità e Rete

32. **È formalizzato un processo di gestione delle vulnerabilità per identificare e prevenire le vulnerabilità tecniche? Ad esempio, vulnerabilità di rete, infrastruttura, architettura:** Si
33. **Sono regolarmente eseguite attività di Penetration Test interne ed esterne?** no, in previsione
34. **L'azienda ha un processo di gestione delle patch in atto?** Si tramite sistemi automatici
35. **Con quale frequenza l'azienda applica le patch di sicurezza?** immediata
36. **Per i sistemi critici e le vulnerabilità critiche è applicata una procedura di patching diversa? In termini di test, valutazione e pianificazione dei tempi di installazione:** Le patch vengono installate automaticamente
37. **L'azienda rinforza i suoi server e workstation e utilizza immagini standardizzate per configurare nuovi sistemi?** si tramite sistema di virtualizzazione e MDT
38. **Quali controlli contro i malware sono implementati dall'azienda?** Controllo tramite Antivirus e MDR
39. **Quali controlli per supportare la protezione della rete sono implementati dall'azienda?** Firewall, VPN, Antivirus
40. **L'azienda ha implementato una segregazione della rete per proteggere i sistemi critici? Ad esempio, DMZ** Si

Ciclo di Vita dello Sviluppo del Sistema

41. **È definita una politica che include regole per lo sviluppo sicuro (ad esempio, pianificazione, progettazione, sviluppo, esecuzione e smaltimento) di software e sistemi?** no - non vengono sviluppati software internamente
42. **Le applicazioni sviluppate sono testate in base a requisiti di sicurezza definiti e vulnerabilità comuni (ad esempio, OWASP Top 10 ecc.)?** non vengono sviluppati software internamente
43. **L'attività di sviluppo del sistema esternalizzato è supervisionata e monitorata? Ad esempio, revisioni di progettazione e codice:** si

Capacità di Logging e Monitoraggio

44. **L'azienda ha un processo di gestione dei log in atto?** è in fase di acquisto software per Log Management
45. **Come gestisce l'azienda i log?** è in fase di acquisto software per Log Management

BYOD (da compilare solo se i dipendenti sono autorizzati ad utilizzare dispositivi personali per l'attività lavorativa)

46. **Esiste un processo per concedere/negare le richieste di autorizzazione all'uso di dispositivi personali?**
47. **L'organizzazione ha una politica BYOD?**
    a. **Include disposizioni che affrontano:**
       requisiti di password/passcode___;
       crittografia___;
       software anti-malware___;
       impostazioni di blocco schermo e cancellazione remota?___
    b. **La politica BYOD afferma che i dipendenti sono responsabili del backup dei dati personali su un dispositivo BYOD per evitare che vengano persi in caso di cancellazione del dispositivo?**
    c. **Informa il dipendente che assume la responsabilità per eventuali danni causati da malfunzionamenti, virus, ecc. del dispositivo BYOD?**
48. **L'organizzazione è autorizzata dai dipendenti a installare un software di gestione dei dispositivi mobili (MDM) sui dispositivi mobili?** no.
49. **Ai dipendenti è vietato intraprendere azioni per aggirare le protezioni di sicurezza messe in atto dall'organizzazione?** Si
50. **I dipendenti sono tenuti a mantenere aggiornati i sistemi operativi e le applicazioni dei dispositivi?** i sistemi si aggiornano tramite GPO
51. **I dipendenti sono tenuti a separare i dati personali dai dati aziendali nella misura massima possibile?** Si
52. **L'organizzazione rende i dipendenti consapevoli dei rischi di sicurezza informatica legati al BYOD? (ad esempio, informando i dipendenti delle loro responsabilità di notificare tempestivamente l'organizzazione in caso di perdita o furto del dispositivo, o se il dispositivo verrà sostituito, aggiornato o venduto; informando i dipendenti di qualsiasi altra impostazione di sicurezza che l'organizzazione intende applicare al dispositivo tramite le sue tecnologie di gestione dei dispositivi mobili, se utilizzate)** Si

Questionario Ransomware

53. **Pre-filtrate le e-mail per allegati e link potenzialmente dannosi?**
- [X] **SÌ**
- [ ] **NO**

54. **Il vostro servizio di filtraggio delle e-mail ha la capacità di detonare automaticamente e valutare gli allegati in un sandbox per determinare se sono dannosi prima della consegna all'utente finale?**
- [ ] **SÌ**
- [X] **NO**

55. **Fornite un servizio di quarantena delle e-mail ai vostri utenti?**
- [ ] **SÌ**
- [X] **NO**

56. **Applicate rigorosamente il Sender Policy Framework (SPF) sulle e-mail in arrivo?**
- [ ] **SÌ**
- [X] **NO**

57. **Con quale frequenza viene condotta la formazione sul phishing a tutto il personale (ad es. mensile, trimestrale, annuale)?**
- [ ] **Mai**
- [X] **Annualmente**
- [ ] **Annualmente e con test di phishing casuali durante l'anno**
- [ ] **Solo al primo assunzione**

58. **I vostri utenti possono accedere alle e-mail tramite un'app web su un dispositivo non aziendale?**
- [X] **SÌ**
- [ ] **NO**

59. **Se gli utenti possono accedere alla posta elettronica aziendale su un dispositivo non aziendale: applicate l'Autenticazione a più fattori (MFA)?**
- [X] **SÌ**
- [ ] **NO**
- [ ] **N/A**

60. **Utilizzate Office 365 nella vostra organizzazione?**
- [ ] **SÌ**
- [X] **NO**

61. **Se utilizzate Office 365: utilizzate il componente aggiuntivo o365 Advanced Threat Protection?**
- [ ] **SÌ**
- [X] **NO**

62. **Utilizzate un prodotto di protezione degli endpoint (EPP) in tutta l'azienda?** Si
63. **Utilizzate un prodotto di rilevamento e risposta degli endpoint (EDR) in tutta l'azienda?** Si

Si prega di indicare la percentuale di workstation coperte da soluzioni EPP/EDR aggiornate: [100% **]**

64. **Utilizzate MFA per proteggere gli account utente?**
- [ ] **SÌ – Solo account privilegiati**
- [ ] **SÌ – Tutti gli account**
- [X] **NO**

65. **È implementata una configurazione di base rinforzata su server, laptop, desktop e dispositivi mobili gestiti?**
- [X] **SÌ**
- [ ] **NO**

66. **Quale percentuale dell'azienda è coperta dalle vostre scansioni di vulnerabilità programmate?** 100

67. **In quale arco di tempo installate patch critiche e di alta gravità in tutta l'azienda?**

- **[ ] Entro 2 settimane**
- **[ ] 1 mese**
- **[ ] 2 mesi**
- **[X] Ad hoc**

68. **Se avete software a fine vita o fine supporto, è segregato dal resto della rete?**

- **[ ] SÌ**
- **[X] NO**
- **[ ] PARZIALMENTE**
- **[ ] Nessuna piattaforma EoL / EoS distribuita**

69. **I vostri utenti hanno diritti di amministratore locale sul loro laptop / desktop?**

- **[ ] SÌ**
- **[X] NO**
- **[ ] Solo una parte degli utenti – Si prega di specificare: _____**

70. **Gestite gli account privilegiati (PAM) utilizzando piattaforme dedicate? Ad esempio, CyberArk**

- **[ ] SÌ**
- **[X] NO**
- **[ ] PARZIALMENTE**

71. **Avete un centro operativo di sicurezza (SOC) istituito, sia interno che esternalizzato?**

- **[ ] SÌ 24/7**
- **[ ] SÌ orario lavorativo**
- **[X] NO**

72. **Conservate una copia dei vostri backup separatamente dalla vostra rete ('offline'), o in un servizio cloud progettato per questo scopo?**

- **[ ] Sì completamente offline**
- **[X] SÌ servizio cloud**
- **[ ] NO**

73. **Le vostre workstation hanno accesso a un servizio di sincronizzazione cloud (ad es. Dropbox, OneDrive, SharePoint, Google Drive) per i backup?**

- **[X] SÌ**
- **[ ] NO**

74. **Avete testato il ripristino e il recupero riuscito delle configurazioni dei server chiave e dei dati dai backup negli ultimi 6 mesi?**

- **[X] SÌ**
- **[ ] NO**
- **[ ] PARZIALE**

75. **Siete in grado di testare l'integrità dei backup prima del ripristino per essere sicuri che siano privi di malware?**

- **[ ] SÌ**
- **[ ] NO**
- **[X] PARZIALE**

76. **Avete condotto esercitazioni o simulazioni di risposta al ransomware negli ultimi 12 mesi?**

- **[X] SÌ**
- **[ ] NO**

77. Avete un playbook di risposta al ransomware documentato o un piano di risposta agli incidenti in atto?

- **[ ] SÌ**
- **[X] NO**

78. Il vostro playbook di risposta al ransomware viene regolarmente rivisto e aggiornato per riflettere le minacce emergenti e i cambiamenti nel vostro ambiente?

- **[ ] SÌ – Annualmente**
- **[ ] SÌ – Senza periodicità programmata**
- **[X] NO**

Altre Misure Preventive contro il Ransomware

79. Si prega di descrivere eventuali ulteriori passaggi che la vostra organizzazione adotta per rilevare e prevenire attacchi ransomware (ad es. segmentazione della rete, strumenti software aggiuntivi, servizi di sicurezza esterni, ecc.):

Sicurezza del Lavoro Agile (SE APPLICABILE)

ACCESSO REMOTO

80. Sono in atto meccanismi di sicurezza per garantire un accesso sicuro alle risorse dell'organizzazione (ad es. VPN)? L'organizzazione adotta metodi di autorizzazione e autenticazione forte? Gli aggiornamenti di sicurezza e le patch sono regolarmente applicati sui sistemi di accesso remoto?

Si

81. Sono adottate soluzioni/strumenti di collaborazione per gestire la comunicazione e la condivisione delle risorse? I livelli di autorizzazione e accesso sono configurati correttamente? Sono aggiornati all'ultima versione?

Si, le autorizzazioni e gli accessi sono configurati correttamente.

82. I dati a riposo/in transito sono crittografati? Sono adottate soluzioni di antispam, anti-spoofing e monitoraggio della rete? Le email sono protette utilizzando ad es. crittografia, anti-spoofing, ecc.?

si per quanto previsto dal provider di posta

83. È possibile monitorare chi e quanti utenti sono connessi alla vostra rete? Cosa stanno accedendo assicurandosi che abbiano il livello di autorizzazione appropriato:

si

SICUREZZA DEI DISPOSITIVI

84. Quali sono le soluzioni di hardening dei dispositivi in atto? (Crittografia, anti-malware, FW, ecc.)?

full disk encription

85. Sono in atto sistemi di gestione della sicurezza e soluzioni di monitoraggio? (MDM, MAM, ecc.)?

in previsione

86. I sistemi operativi e le applicazioni dei dispositivi sono aggiornati? Le patch di sicurezza sono applicate tempestivamente?

Si, applicate tempestivamente

GESTIONE DEL RISCHIO PANDEMICO

87. La strategia di rischio fornisce istruzioni per gestire i rischi IT e di sicurezza durante l'emergenza?

non applicabile

88. Il Piano di Gestione degli Incidenti considera i rischi di sicurezza informatica derivanti dall'emergenza

Coronavirus?
non applicabile.

89. **Sono in atto software/strumenti di monitoraggio degli eventi di sicurezza, specialmente per i sistemi critici? Sono integrati con la strategia di gestione del rischio di terze parti?**
non applicabile

90. **Sono in atto processi di escalation o procedure di comunicazione per informare chiaramente i clienti sugli incidenti/breaches di sicurezza causati dalla pandemia?**
non applicabile

RESILIENZA AZIENDALE

91. **L'organizzazione considera nella sua strategia di Continuità Operativa la gestione della pandemia?**
non applicabile

92. **Il piano pandemico considera la maggior parte degli scenari possibili (ad es. indisponibilità del personale; arresto dei sistemi; restrizioni governative, ecc.)? Il piano pandemico stabilisce ruoli e responsabilità per la gestione della continuità operativa, specialmente per le comunicazioni con i clienti e i fornitori?**
non applicabile

93. **Le risorse sono costantemente monitorate per mantenere l'adeguata disponibilità dei sistemi IT?**
si.

CONSAPEVOLEZZA

94. **Esiste una politica di sicurezza specifica relativa ai rischi del lavoro agile disponibile per tutti i dipendenti?**
non applicabile

95. **L'organizzazione fornisce campagne di sensibilizzazione specifiche che spiegano tutti i rischi informatici legati all'emergenza pandemica per tutti i dipendenti (phishing, minacce informatiche, ecc.)?** non applicabile

Storia sinistri

96. **Negli ultimi 5 anni, la Contraente ha mai subito una violazione intenzionale della sicurezza IT, danni alla rete, interruzione dell'attività o danneggiamento del sistema?**
    a. **In caso positivo si prega di fornire:**
       Data e descrizione puntuale dell'evento;
       Danno economico eventualmente subito;
       Migliorie attuate per evitare che riaccada;

No

97. **Un Cliente o altra persona od entità ha affermato che i propri dati personali sono stati compromessi dalla contraente o da qualsiasi fornitore di servizi che elabora, tratta o raccoglie dati personali per conto della Contraente? Se s' si prega di fornire dettagli** No
98. **La Contraente ha mai informato una persona che le sue informazioni sono state o potrebbero essere state compromesse? Se sì si prega di fornire:**
    a. **Data e descrizione puntuale dell'evento;**

b. Danno economico eventualmente subito;

c. Migliorie attuate per evitare che riaccada;

no

99. La Contraente è a conoscenza di informazioni su qualsiasi fatto, circostanza, situazione, evento o transazione che possano originare una richiesta di risarcimento o notifica di violazione della privacy? Se sì, fornire i dettagli no

Il Referente per la Cybersicurezza
Dott. Fausto Pitzalis
ARST SpA