

Modulo di proposta

Le risposte per la Cyber Risk Evaluation Enterprise Edition di Aon

Informazioni Profilo			
Nome dell'azienda		Agenzia Regionale per la Prevenzione e Protezione Ambientale del Veneto	
Etichetta di valutazione definita dall'utente		Luca Menini	
Versione di valutazione		5.10	
Contatto	Luca Menini	Ruolo	dirigente
Email		luca.menini@arpa.veneto.it	
Settore dell'Organizzazione		Natural Resources.Power Generation & Distribution	
Inoltrato		5 giu 2026	
Ricavi Annuali	\$ 50,000	Bilancio IT	
Utile lordo annuo		% di budget nella sicurezza IT	
Organico		Numero di dipendenti	
		Organico della sicurezza	

Informazioni sul numero dell'assicurato	
Indirizzo del Nome dell'assicurato	via Ospedale Civile 24
Città del Nome dell'assicurato	Padova
Stato del Nome dell'assicurato	---
Paese del Nome dell'assicurato	Italy
Codice Postale del Nome dell'assicurato	35100

Critical Systems and Data

Overview

1.1.1 Quanto è centralizzato il programma di sicurezza informatica dell'organizzazione?

- La sicurezza delle informazioni dell'organizzazione è gestita a livello centrale e le policy si applicano a tutti i processi. Quando vengono fatte eccezioni, è solo per asset (invece che per operazione/entità legale).

La sicurezza delle informazioni dell'organizzazione è gestita a livello centrale, ma sono previste eccezioni per alcuni processi/entità legali. I controlli delineati nel CyQu e negli eventuali questionari aggiuntivi si applicano a più o meno il 98% degli endpoint totali.

La sicurezza delle informazioni dell'organizzazione è gestita a livello centrale, ma sono previste eccezioni per alcuni processi/legali. I controlli delineati nel CyQu e negli eventuali questionari aggiuntivi si applicano a meno del 98% degli endpoint totali.

La sicurezza delle informazioni dell'organizzazione è federata, ma i controlli delineati in CyQu e negli eventuali questionari aggiuntivi si applicano a più o meno il 98% degli endpoint totali.

La sicurezza delle informazioni dell'organizzazione è federata e i controlli delineati in CyQu e negli eventuali questionari aggiuntivi si applicano a più del 50% degli endpoint totali, ma a meno del 98% degli endpoint totali.

La sicurezza delle informazioni è gestita da singole entità legali o unità operative. I controlli riportati di seguito si basano su un'indagine condotta su tutte le entità e le unità operative.

Architecture

1.2.1 Numero di data center interni 1

1.2.2 Dove sono ubicati i data center interni? Teolo

1.2.3 Numero di data center esterni (es. off-premise, cloud, co-location): 2

1.2.4 Dove sono ospitati i data center esterni? Padova c/o Infocamere e Polo Strategico Regionale (Regione veneto)

1.2.5 Numero di server (on premise): 15

1.2.6 Numero di server (virtuali): 210

1.2.7 Numero di workstation, compresi laptop, desktop, macchine virtuali e sistemi di punti vendita (PoS) : 1100

1.2.8 Numero di dispositivi OT, tra cui controllori logici programmabili (PLC), sistemi di controllo industriale (ICS) e sistemi di controllo distribuiti (DCS): 0

1.2.9 Numero di dispositivi mobili, tra cui telefoni e tablet: 700

1.2.10 In quali regioni opera la vostra organizzazione? (selezionare tutte le voci applicabili)

- ☐ Australia e Nuova Zelanda
- ☐ Canada
- ☐ Asia centrale e meridionale
- ☐ Asia orientale e Pacifico
- ☒ Europa
- ☐ Messico, America Centrale e Caraibi
- ☐ Medio Oriente e Nord Africa
- ☐ Russia
- ☐ Sud Africa

☐ Sud America

☐ Stati Uniti

1.2.11 Processi e/o Applicazioni critici per il Business: (Selezionare tutte le voci applicabili)

- ✓ Sistema di Gestione Documentale
- ✓ Processo di Pagamento
- ✓ Finanza (buste paga, contabilità fornitori)
- ✓ Risorse Umane (HR)
- ✓ E-mail/Comunicazioni
- ✓ Pianificazione delle Risorse Aziendali (ERP - Enterprise Resource Planning)/Gestione della Catena di Approvvigionamento (Supply Chain)
- ☐ Gestione della Relazione coi Clienti (CRM - Customer Relationship Management)
- ☐ Sistema di Cartelle Cliniche Elettroniche (EHR - Electronic Health Record)
- ☐ Data Lake
- ☐ Nessuno dei precedenti

1.2.12 Dispositivi Internet of Things presenti (Selezionare tutte le voci applicabili)

- ☐ Apparecchiature sanitarie
- ✓ Asset industriali (IIoT)
- ☐ Dispositivi indossabili
- ☐ Veicoli / Flotta
- ☐ Gestione degli edifici
- ☐ Nessuno dei precedenti

1.2.13 Sistemi di Controllo Industriale (ICS- Industrial Control System) presenti: (Selezionare tutte le voci applicabili)

- ☐ Sistemi SCADA
- ☐ Sistemi di Controllo Distribuito (DCS - Distributed Control Systems)
- ☐ Controllori Logici Programmabili (PLC - Programmable Logic Controllers)
- ✓ Sistema di Produzione
- ☐ Nessuno dei precedenti

1.2.14 Fornitori esterni critici (Selezionare tutte le voci applicabili)

- ☐ Data Center Condivisi
- ☐ Data Center Dedicati
- ☐ Disaster Recovery
- ☐ Elaborazione Dati
- ☐ Desktop come Servizio (es. Thin Client o Remote Workstation Desktop)
- ☐ Domain Name Services (DNS)
- ✓ Infrastruttura come Servizio (IaaS) come ad esempio VMware Vcenter, MS Azure, o altri sistemi di virtualizzazione delle infrastrutture informatiche
- ☐ Gestione del Fornitore dei Servizi di Sicurezza
- ☐ Piattaforma come Servizio (PaaS) ovvero un insieme di Sistemi per sviluppare, testare, implementare e mantenere applicazioni da un ambiente di sviluppo integrato di base (es. Cloud Foundry, AWS, IBM Cloud computing, etc.)
- ☐ Logistica
- ☐ Gestione delle Relazioni coi Clienti (CRM)
- ✓ Risorse Umane (HR)
- ☐ eCommerce
- ☐ Nessuno dei precedenti

1.2.15 Indicare l'utilizzo da parte dell'organizzazione di Microsoft Active Directory (in tutti i domini/foresta) e Office 365; selezionare tutte le opzioni applicabili:

- ☐ L'organizzazione utilizza Office 365
- ☐ L'organizzazione utilizza le best practice di PowerShell come indicato da Microsoft.
- ☒ L'organizzazione utilizza Microsoft Active Directory
- ☐ Nessuno dei precedenti

Sensitive and Confidential Data

1.3.1 L'organizzazione PCI DSS 3.x è certificata come livello Merchant definito?

- Si
- No

1.3.2 A cosa hanno accesso i dipendenti quando lavorano in remoto?

Non disponibile: i dipendenti non possono accedere a dati o sistemi in remoto

Accesso solo a soluzioni SaaS esterne

Soluzione per applicazioni virtuali e desktop, con accesso limitato a dati e sistemi interni/esterni

- Soluzione per applicazioni virtuali e desktop, con accesso completo ai dati aziendali, ai sistemi interni ed esterni

Data Security

Data Classification

2.1.1 La vostra organizzazione classifica i propri dati per identificare ulteriori controlli atti a salvaguardare le informazioni? (ad esempio, informazioni di identificazione personale, proprietà intellettuale, dati sanitari)

- Il processo non è adeguatamente implementato
 - I dati vengono classificati come un'operazione unica, e/o includono alcuni casi d'uso
 - I dati vengono classificati regolarmente, e includono tutti i casi d'uso
 - I dati vengono classificati regolarmente, durante cambi significativi, e includono tutti i casi d'uso

User Awareness and Training

2.2.1 Come viene definito il vostro programma di formazione sulla privacy dei dati e sulla sicurezza informatica?

- Nessun utente riceve una formazione di sensibilizzazione alla sicurezza
- Gli utenti ricevono una formazione di sensibilizzazione alla sicurezza, ma non è obbligatoria in tutta l'organizzazione
 - Tutti gli utenti ricevono una formazione obbligatoria sulla sicurezza informatica entro 30 giorni dall'ingresso nell'organizzazione e ricevono una formazione aggiuntiva obbligatoria sull'awareness ogni anno. La formazione si basa sui ruoli e sulle responsabilità specifiche degli utenti (ad esempio, gruppi di accesso elevati).
 - Tutti gli utenti ricevono una formazione obbligatoria sulla sicurezza informatica entro 30 giorni dall'ingresso nell'organizzazione e ricevono una formazione aggiuntiva obbligatoria sull'awareness ogni anno.

2.2.2 Il vostro Programma di Sensibilizzazione alla Sicurezza include quanto segue? Selezionare tutte le voci applicabili.

- ☒ L'importanza di attivare e utilizzare l'autenticazione sicura
- ☒ Come identificare le differenti forme di attacchi di ingegneria sociale, come il phishing, le truffe telefoniche e l'impersonificazione telefonica
- ☒ Come identificare conservare, trasferire, archiviare e distruggere in maniera appropriata le informazioni sensibili

- ✓ Cause comuni per l'esposizione non intenzionale dei dati, come la perdita di dispositivi o l'invio di e-mail alla persona sbagliata a causa del completamento automatico delle e-mail
- [] Indicatori comuni di un incidente e il processo per la relativa denuncia
- ✓ L'importanza di tenere le password riservate
- ✓ I rischi dell'utilizzo di password già utilizzate
- ✓ L'importanza di implementare buone pratiche di sicurezza fisica (ad es. impedire assembramenti, bloccare estranei senza badge, etc.)
- ✓ Responsabilità per coloro che hanno permessi di accesso privilegiati
- [] Nessuno dei precedenti

2.2.3 Vengono condotte esercitazioni di social engineering o phishing come parte di un programma di sensibilizzazione continuo?

Controllo non implementato

Sì, condotto su una base ad-hoc con un feedback limitato

Sì, condotto su base regolare (ad esempio mensilmente) con qualche feedback

- Sì, condotto su base regolare con feedback condivisi direttamente con i dipendenti e collegato a un programma di consapevolezza più ampio (ad es. formazione obbligatoria su computer per numero di visitatori elevato su esercizi di phishing)

Data Protection

2.3.1 Proteggete tutte le informazioni sensibili in archivio?

- I dati in archivio non sono crittografati
- I dati in archivio sono crittografati manualmente
- I dati a riposo vengono crittografati automaticamente

2.3.2 Proteggete le informazioni sensibili durante la loro trasmissione?

- I dati non sono crittografati durante la trasmissione
- I dati sono crittografati manualmente durante la trasmissione
- I dati in transito vengono crittografati automaticamente

Governance

2.4.1 Il Consiglio di Amministrazione e il Top Management hanno una chiara visione sull'importanza della Cybersecurity?

Non c'è alcuna comunicazione sulle aspettative o sull'importanza della cybersecurity da parte del Consiglio di Amministrazione e del Top Management

- Si fanno riferimenti limitati alla cybersecurity in comunicazioni ufficiali del Consiglio di Amministrazione e del Top Management

Le aspettative della leadership sono chiaramente espresse e comunicate in modo coerente per creare una visione comune sull'importanza della cybersecurity

Il Consiglio di Amministrazione e la direzione esecutiva hanno una chiara visione sull'importanza della cybersecurity che è coerente, visibile e realizzato in modo duraturo

2.4.2 Un Comitato competente (con un controllo di gestione del rischio o responsabilità di revisione) riceve report di cybersecurity che includono quanto segue? Selezionare tutte le voci applicabili.

- ✓ Minacce principali e relative contromisure/attività di cybersecurity
- ✓ Incidenti cyber e le collegate cause principali
- [] Responsabilità collegate alla Proprietà (titolari)
- ✓ Roadmap, piani d'azione e relativo stato di avanzamento

- ☐ Indicatori di Rischio Principali, limiti di tolleranza e soglie di carattere finanziario
- ✓ Metriche e tendenze delle prestazioni di Cybersecurity
- ✓ Informazioni sulle minacce emergenti
- ☐ Nessuno dei precedenti

2.4.3 Quanto spesso il Comitato riceve report sul profilo di rischio cyber dell'organizzazione?

Raramente

Annualmente

- Almeno due volte all'anno

Ogni trimestre o più frequentemente

2.4.4 Esiste un referente aziendale di livello executive (ad esempio, CTO, CIO, CISO, GC) per promuovere la sicurezza informatica o ruoli dedicati con responsabilità per la sicurezza informatica?

Non esiste un referente di livello executive che promuova la sicurezza informatica o ruoli dedicati con responsabilità per la sicurezza informatica.

- Esiste un ruolo dedicato a livello manageriale che è responsabile della sicurezza informatica (ad esempio, il responsabile della sicurezza delle informazioni, il responsabile della sicurezza dei dati o il responsabile della protezione dei dati).

Esiste un referente di livello executive che promuove la sicurezza informatica (ad esempio, CTO, CIO, CFO, CxO).

Esiste un referente di livello executive nel consiglio di amministrazione per promuovere la sicurezza informatica (ad es. CTO, CIO, CFO, CxO).

Risk Management

2.5.1 C'è collaborazione fra le principali funzioni competenti sulla cyber security che includano l'Audit Interno, l'Information Technology, la Sicurezza, il Legale / Compliance, il Risk Management e la Business Continuity per stimare e gestire i rischi cyber?

Raramente o mai

- Alcuni gruppi collaborano su base occasionale (ad es. limitati a uno o due team, o su base reattiva)

Sì, c'è collaborazione formale e costante tra le funzioni

Sì, c'è collaborazione formale, costante che include l'applicazione di una metodologia comune per la valutazione del rischio, di tecniche di quantificazione finanziaria, nonché l'approccio alla gestione del rischio con report periodici al Top Management

2.5.2 Come è impegnato il leader senior di Cybersecurity durante le revisioni di decisioni strategiche che includono investimenti di capitale significativi, nuovi ingressi sul mercato, sviluppo di nuovi prodotti o attività di M&A? Selezionare tutte le voci applicabili

- ☐ Fornisce opinioni riguardanti i rischi prima che venga presa una decisione
- ☐ Fornisce opinioni riguardanti i rischi dopo che è stata presa una decisione
- ☐ Contribuisce alla valutazione dell'impatto commerciale sul profilo di rischio del business aziendale
- ☐ Fornisce suggerimenti per le strategie di mitigazione del rischio e piani d'azione una volta presa una decisione
- ✓ Nessuno dei precedenti

2.5.3 Vengono valutate raccomandazioni per la cybersecurity utilizzando metriche finanziarie e da una prospettiva di Ritorno da un Investimento in Sicurezza (ROSI)?

- Mai o limitato a metriche semi-quantitative

I suggerimenti sono valutati in determinate circostanze, ma senza utilizzare un approccio uniforme

I suggerimenti sono valutati in modo coerente

I suggerimenti sono valutati in modo coerente utilizzando metriche finanziarie che sono allineate alla propensione al rischio e alle soglie di tolleranza

2.5.4 Per quanto riguarda le politiche dell'organizzazione per l'uso degli asset organizzativi, selezionare tutte quelle che si applicano:

- ☐ L'organizzazione dispone di una "Politica di utilizzo accettabile" (AUP) che definisce gli obblighi e i vincoli degli utenti.
- ☐ La AUP descrive le conseguenze delle violazioni della policy
- ☒ Agli utenti non è consentito navigare su piattaforme di social media dalle risorse dell'organizzazione, a meno che non si tratti di un'esigenza aziendale definita.
- ☐ Agli utenti non è consentito accedere alla posta elettronica personale dalle risorse organizzative.
- ☐ Agli amministratori è esplicitamente vietato navigare in Internet o accedere alla posta elettronica personale con i loro account privilegiati.
- ☒ Gli utenti e gli amministratori sono responsabili di mantenere il proprio computer e i propri account al sicuro da rischi o problemi comuni.
- ☒ La politica incoraggia o richiede agli utenti e agli amministratori di segnalare le violazioni sospette.
- ☐ Nessuno dei precedenti

Access Control

Access Management

3.1.1 Si limitano i diritti di accesso dell'amministratore? (ad esempio, ID separato per l'amministratore, internet/e-mail, amministratore locale)

- I diritti di accesso a livello di amministratore non sono limitati
- I diritti di accesso a livello di amministratore sono limitati per alcuni sistemi
- I diritti di accesso a livello di amministratore sono limitati per tutti i sistemi
- I diritti di accesso a livello di amministratore sono limitati per tutti i sistemi basati sul rischio di privilegi elevati

3.1.2 Ricertificate i diritti di accesso, considerando la separazione delle funzioni, a intervalli regolari?

- La ricertificazione dei diritti di accesso non avviene
- La ricertificazione dei diritti di accesso è manuale o avviene solo per alcuni sistemi
- La ricertificazione dei diritti di accesso è automatizzata e avviene per tutti i sistemi almeno una volta all'anno.
- La ricertificazione dei diritti di accesso è automatizzata e avviene per tutti i sistemi con cadenza almeno trimestrale.

3.1.3 Utilizzate un tool automatico per la creazione o cancellazione di una identità?

- Nessun tool automatico al momento viene impiegato
- Un tool automatico copre alcuni sistemi (applicazioni, server, database, active directory, unità di rete)
- Un tool automatico copre tutti i sistemi
- Un tool automatico copre tutti i sistemi e viene aggiornato per adeguarsi ai rischi emergenti almeno una volta l'anno

3.1.4 Revocate tempestivamente l'accesso per i dipendenti agli account, ai servizi e ai sistemi, alla cessazione dal cambiamento del rapporto lavorativo o del ruolo in azienda?

- L'accesso non viene revocato
- L'accesso viene revocato in un modo ad-hoc conseguentemente ad una notifica di un manager o un HR preposto
- L'accesso viene revocato in modo coerente dal team IAM in caso di notifica di licenziamento o di cambio di ruolo entro 24 ore.
- L'accesso viene revocato automaticamente alla notifica di cessazione o al cambio di ruolo attraverso script/strumenti automatici entro 24 ore.

3.1.5 Prevedete un audit sui log delle modifiche ai gruppi di amministratori, incluse le aggiunte, le modifiche, le rimozioni e gli accessi non riusciti?

- Non sono mai previsti audit dei log
- Sono previsti audit dei log per alcuni sistemi

Sono previsti audit dei log per tutti sistemi

Sono previsti audit dei log per tutti i sistemi e vengono monitorati sulla base del rischio dei gruppi di amministratori

3.1.6 Mettete in atto controlli di accesso su documenti conservati nelle seguenti ubicazioni? Selezionare tutte le voci applicabili.

- ☒ File System
- ☒ Condivisioni di Rete
- ☒ Applicazioni
- ☒ Database
- ☐ Nessuno dei precedenti

3.1.7 Per quanto riguarda il modo in cui l'organizzazione protegge gli account utente con privilegi amministrativi di dominio ("Account amministratore di dominio"), selezionare tutte le opzioni applicabili:

- ☒ Gli amministratori di sistema dell'organizzazione dispongono di una credenziale unica e privilegiata per le attività amministrative (separata dalle credenziali utente per l'accesso quotidiano, la posta elettronica, ecc.)
- ☐ Gli account amministratore di dominio sono gestiti e monitorati attraverso l'accesso just-in-time, sono limitati nel tempo e richiedono approvazioni per fornire accesso privilegiato.
- ☐ Le credenziali degli "Account amministratore di dominio" sono conservate con una password sicura che richiede all'utente di "estrarre" le stesse credenziali (che vengono ruotate in seguito).
- ☐ Oltre ad essere conservati con una password sicura, gli "Account amministratore di dominio" non vengono esposti all'utente amministratore quando vengono "estratti" e l'accesso viene registrato tramite un gestore di sessione.
- ☒ Esiste un registro di tutte le azioni compiute dagli "account amministratore di dominio" per almeno gli ultimi trenta giorni.
- ☐ Gli account amministratore di dominio possono essere utilizzati solo da postazioni di lavoro ad accesso privilegiato (postazioni di lavoro che non hanno accesso a Internet o alla posta elettronica).
- ☐ Nessuno dei precedenti

3.1.8 Per quanto riguarda il modo in cui l'organizzazione protegge gli "account di servizio" "con permessi privilegiati", selezionare tutte le opzioni applicabili:

- ☐ Esiste un inventario di tutti gli account di servizio privilegiati, che viene aggiornato almeno trimestralmente.
- ☐ Gli account di servizio privilegiati hanno password di almeno 25 caratteri.
- ☐ Le password degli account di servizio privilegiati vengono ruotate almeno una volta all'anno.
- ☐ Gli account di servizio privilegiati hanno una rotazione delle password almeno trimestrale.
- ☒ Gli account di servizio sono suddivisi in livelli, in modo che vengano utilizzati account diversi per interagire con le postazioni di lavoro, i server e i server di autenticazione, anche per lo stesso servizio.
- ☐ Viene utilizzata una soluzione di Privileged Access Management (PAM) per gestire le password e l'accesso agli account privilegiati.
- ☐ L'organizzazione ha configurato tutti gli account di servizio per negare i login interattivi.
- ☒ È in atto un processo di revisione almeno annuale dei requisiti attuali per ciascun servizio associato agli account di servizio privilegiati, per verificare che il servizio richieda ancora i permessi di cui dispone l'account di servizio (e privarlo dei privilegi in caso contrario).
- ☐ Nessuno dei precedenti

3.1.9 Numero di account utente nel gruppo Domain Admin (inclusi gli account di servizio): 1

3.1.10 Numero di account di servizio privilegiati: 20

3.1.11 Commento aggiuntivo sul numero di Amministratori di Dominio (Domain Admin) :

numero minimo necessario

3.1.12 L'organizzazione dispone di un inventario di tutti gli account utente ed utenze amministrative?

- Sì
- No

3.1.13 L'inventario degli account dell'organizzazione include il nome dell'individuo, il nome utente, le date di inizio/arresto e il reparto?

- Sì
- No

3.1.14 Quali criteri di audit sono abilitati sui controller di dominio dell'organizzazione? Selezionare tutte le opzioni applicabili.

- ☐ Convalida delle credenziali di audit (fallimento)
- ☐ Creazione di processi di audit (successo)
- ☐ Gestione dei gruppi di sicurezza (successo e fallimento)
- ☐ Controllo della gestione degli account utente (successo e fallimento)
- ☐ Audit di altri eventi di gestione degli account (successo e fallimento)
- ☐ Audit dell'uso di privilegi sensibili (successo e fallimento)
- ☐ Audit dell'accesso (successo e fallimento)
- ☐ Verifica degli accessi speciali (successo)
- ☒ Nessuno dei precedenti/non so

- Commenti: non sono previsti audit interni

3.1.15 Per quanto riguarda i controlli di accesso per le workstation di ciascun utente, selezionare tutte le opzioni applicabili:

- ☒ Nessun dipendente, ad eccezione degli amministratori IT, fa parte del gruppo Administrators o ha accesso come amministratore locale alle proprie postazioni di lavoro.
- ☒ La politica dell'organizzazione prevede che i dipendenti non facciano parte del gruppo degli amministratori e non abbiano accesso all'amministrazione locale; tutte le eccezioni alla politica sono documentate.
- ☒ Alcuni dipendenti dell'organizzazione fanno parte del gruppo Administrators o sono amministratori locali.
- ☒ Viene utilizzato Microsoft Local Administrator Password Solution (LAPS) o un software simile per la gestione delle credenziali degli account amministrativi locali
- ☒ Le credenziali dell'account amministratore locale sono le stesse su più computer e/o server.
- ☐ Nessuno dei precedenti

3.1.16 Per quanto riguarda i controlli di accesso per i server, selezionare la descrizione che meglio riflette la postura dell'organizzazione. Questa domanda riguarda gli account utente quotidiani dei dipendenti; se l'organizzazione fornisce ai dipendenti credenziali separate per l'accesso amministrativo, tali account non devono essere considerati ai fini della presente domanda.

- Nessun dipendente fa parte del gruppo degli amministratori o ha accesso come amministratore locale ai server membri.
La politica dell'organizzazione prevede che i dipendenti non facciano parte del gruppo degli amministratori e non abbiano accesso all'amministrazione locale; tutte le eccezioni alla politica sono documentate.
Alcuni dipendenti dell'organizzazione fanno parte del gruppo degli amministratori o sono amministratori locali.
Non so

3.1.17 Quanti utenti dell'organizzazione hanno accesso amministrativo persistente a server e/o workstation diversi dai propri? 7

Password Configuration

3.2.1 Sono standard le seguenti configurazioni delle password in tutto l'ambiente tecnologico che include l'active directory, le applicazioni, i server, i database, e gli endpoint? Selezionare tutte le voci applicabili.

- ☒ Le configurazioni delle password richiedono un intervallo di scadenza
- ☒ Le configurazioni delle password richiedono una complessità di almeno 10 caratteri per gli account standard e 12 caratteri per gli account privilegiati.
- ☒ Le configurazioni delle password richiedono un blocco su tentativi ripetuti
- ☒ Le configurazioni delle password non permettono di riutilizzare password precedenti

☐ Esiste una soluzione per impedire agli utenti di impostare password comuni e note, anche se soddisfano i requisiti di complessità (come "Passw0rd!").

☐ Nessuno dei precedenti

3.2.2 Cambiate password di default per i seguenti sistemi? Selezionare tutte le voci applicabili.

- ✓ Applicazioni
- ✓ Server
- ✓ Database
- ✓ Firewall
- ✓ Punti di Accesso Wireless
- ✓ Device e sistemi OT (ad es. ICS and SCADA device se applicabili)
- ✓ Device IOT (se applicabili)
- ☐ Nessuno dei precedenti

Multi-Factor Authentication

3.3.1 Mettete in atto l'identificazione unica (SingleSignOn) per le vostre applicazioni di sistema?

L'SSO non è implementata

- L'SSO è implementata ma non include tutti gli accessi critici come amministratore

L'SSO è implementata e include tutti gli accessi critici come amministratore

L'SSO viene distribuito, include tutti gli accessi amministrativi critici ed è aggiornato per allinearsi alle minacce emergenti del settore

3.3.2 È richiesta l'autenticazione a più fattori per l'amministratore e l'accesso privilegiato?

- Controllo non implementato

Sì, in alcuni casi

Sì, nella maggior parte dei casi e le eccezioni sono documentate

Sì, in tutti i casi

3.3.3 È richiesta l'autenticazione a più fattori per accedere a informazioni critiche?

- Controllo non implementato

Sì, in alcuni casi

Sì, nella maggior parte dei casi e le eccezioni sono documentate

Sì, in tutti i casi

3.3.4 È richiesta l'autenticazione a più fattori per l'accesso remoto?

- Controllo non implementato

Sì, in alcuni casi

Sì, nella maggior parte dei casi e le eccezioni sono documentate

Sì, in tutti i casi

3.3.5 È richiesta l'autenticazione a più fattori per accedere ai dispositivi personali?

- Controllo non implementato

Sì, in alcuni casi

Sì, nella maggior parte dei casi e le eccezioni sono documentate

Sì, in tutti i casi

3.3.6 È richiesta l'autenticazione a più fattori per accedere alle risorse cloud?

Controllo non implementato

- Sì, in alcuni casi

Sì, nella maggior parte dei casi e le eccezioni sono documentate

Sì, in tutti i casi

3.3.7 Se l'MFA è richiesto per l'accesso remoto e privilegiato, quali sono i secondi fattori utilizzati? Selezionare tutti quelli che si applicano.

☒ SMS

☐ Biometrico

☐ Applicazione basata su

☐ Token hardware

☐ Altro - fornire ulteriori dettagli nei commenti

3.3.8 Come fanno i terzi ad accedere da remoto alla rete dell'organizzazione?

Le terze parti ricevono account utente permanenti con solo un nome utente e una password per l'autenticazione.

- Alle terze parti vengono assegnati user account permanenti e l'MFA è richiesto per alcuni tipi di accesso remoto alla rete

Alle terze parti vengono forniti user account permanenti e l'MFA è richiesto per la maggior parte degli accessi remoti alla rete aziendale, con eccezioni documentate.

Le terze parti ricevono user account permanenti e l'MFA è richiesto per tutti gli accessi remoti alla rete aziendale.

Alle terze parti viene concesso un accesso "just in time" alla rete con token o password che scadono entro 6 ore.

Alle terze parti viene concesso l'accesso "just in time" alla rete con token o password che scadono dopo più di 6 ore

Non viene fornito alcun accesso remoto a terzi

Endpoint and Systems Security

Endpoint Protection

4.1.1 Utilizzate la crittografia dell'intero disco (ad es. laptop/desktop/mobile)?

Controllo non implementato

- La crittografia del disco viene impiegata per alcuni endpoint

La crittografia del disco viene impiegata per tutti gli endpoint

La crittografia del disco viene impiegata per tutti gli endpoint e viene aggiornata per adeguarsi alla tecnologia con i rischi emergenti (ad es.: IoT)

4.1.2 Per quanto riguarda la sicurezza degli endpoint delle workstation (desktop e portatili), selezionare tutte le opzioni applicabili:

☒ La politica dell'organizzazione prevede che tutte le postazioni di lavoro siano dotate di antivirus con funzionalità euristiche.

☒ L'organizzazione utilizza strumenti di sicurezza degli endpoint con capacità di rilevamento comportamentale e di mitigazione degli exploit.

☒ Le postazioni di lavoro dell'organizzazione utilizzano una configurazione di base rinforzata.

☒ L'organizzazione dispone di un gruppo interno che monitora l'output degli strumenti di sicurezza degli endpoint e indaga su eventuali anomalie.

☐ L'organizzazione dispone di un gruppo esterno che monitora l'output degli strumenti di sicurezza degli endpoint e indaga su eventuali anomalie.

☐ Il software di gestione delle password è disponibile per gli utenti sulle postazioni di lavoro dell'organizzazione.

☐ L'organizzazione ha una politica che prevede che tutti i dispositivi portatili utilizzino la crittografia completa del disco.

☐ Nessuno dei precedenti

4.1.3 La soluzione di protezione dal malware è in grado di fornire funzionalità forensi per la risposta agli incidenti e/o la riparazione?

- Controllo non implementato

Viene configurato un software endpoint per fornire capacità d'indagine su alcuni device inclusi smartphone, tablet, laptop, desktop, etc.

Viene configurato un software endpoint per fornire capacità d'indagine su tutti i device

Viene configurato un software endpoint per fornire capacità d'indagine su tutti i device e viene aggiornato regolarmente con le firme recenti

4.1.4 Indica il fornitore di Endpoint Detection & Response (EDR): TrendMicro

4.1.5 Indica il prodotto EDR utilizzato: ApexOne

4.1.6 In quale percentuale di workstation e server è applicata la protezione degli endpoint: 100

4.1.7 A quale percentuale di dispositivi mobili (compresi tablet, smartphone, ecc.) è applicata la protezione degli endpoint? 0

4.1.8 Per quanto riguarda la configurazione degli strumenti di sicurezza degli endpoint descritti in precedenza, selezionare tutte le opzioni applicabili:

- ✓ Gli strumenti sono configurati in modo da bloccare (e non solo notificare) i processi/file sospetti e dannosi
- ✓ Gli strumenti sono stati messi a punto per l'ambiente dell'organizzazione.
- ✓ Per gli strumenti che richiedono definizioni aggiornate, tali strumenti vengono aggiornati almeno quotidianamente.
- ✓ Le funzioni anti-manomissione sono abilitate
- ☐ Gli strumenti monitorano gli indicatori di minaccia; identificano schemi che corrispondono a minacce note; rispondono automaticamente rimuovendo o contenendo le minacce; avvisano il personale di sicurezza degli incidenti; forniscono capacità di analisi forense e analisi per consentire agli analisti di svolgere attività di caccia alle minacce.
- ☐ Nessuno dei precedenti

4.1.9 Commento aggiuntivo sulle funzionalità di sicurezza degli endpoint:

4.1.10 Utilizzate soluzioni di sicurezza basate sul cloud con le seguenti caratteristiche per il filtraggio del Domain Name System (DNS)? Selezionare tutte le opzioni applicabili.

- ✓ Impedisce agli utenti di visitare siti malevoli
- ✓ Controlla le pagine web per gli URL in base al contenuto
- ✓ Rileva e previene le comunicazioni del centro di comando e controllo per gli endpoint interessati da ransomware
- ✓ Bloccare i download noti come dannosi o sospetti, compresi gli eseguibili.
- ☐ Bloccare i domini non classificati e di recente registrazione utilizzando proxy web o filtri DNS.
- ☐ Nessuno dei precedenti

4.1.11 La sicurezza della Mail prevede le seguenti misure; seleziona tutte le risposte pertinenti:

- ✓ Prescreening delle e-mail per gli allegati e i link potenzialmente dannosi oltre all'indicazione formale quando il destinatario è esterno.
- ✓ L'organizzazione richiede l'autenticazione a più fattori per consentire agli utenti di accedere all'email aziendale
- ✓ L'organizzazione utilizza un componente aggiuntivo di protezione avanzata da minacce via email
- ☐ Servizio di quarantena per e-mail sospette
- ☐ Possibilità di detonare e valutare automaticamente allegati e link in una sandbox
- ✓ Applicazione del Sender Policy Framework (SPF) alle e-mail in entrata
- ✓ Conduce attacchi di phishing simulati contro i dipendenti (se oltre il 15% dei dipendenti fallisce, condividi i dettagli di seguito)
- ✓ L'organizzazione dispone di un processo documentato per rispondere alle campagne di phishing
- ✓ Formazione di awareness alla sicurezza informatica condotta con tutto il personale almeno una volta all'anno
- ✓ Una procedura che consente ai dipendenti di segnalare e-mail sospette alle risorse di sicurezza informatica per indagare
- ✓ I protocolli di posta elettronica tradizionali che utilizzano l'autenticazione di base (solo nome utente e password), come IMAP, POP3 e SMTP, sono disabilitati.
- ☐ L'esecuzione delle macro di MS Office è disabilitata sui documenti per impostazione predefinita
- ☐ Gli utenti non possono abilitare le macro
- ☐ È configurata la posta identificata con chiavi di dominio (DKIM).

- ☐ Domain Based Message Authentication, Reporting and Conformance (DMARC) configurato per rifiutare le e-mail da mittenti sconosciuti ("p=reject").
- ☐ Nessuno dei precedenti

Vulnerability Management

4.2.1 Eseguite scansioni automatiche per rilevare le vulnerabilità es. attività di Vulnerability Assessment?

Controllo non implementato

Le scansioni automatiche coprono solo alcuni asset e/o non seguono gli accordi sui livelli di servizio (SLA) predefiniti per la bonifica.

- Le scansioni automatiche coprono tutti gli asset e seguono SLA di ripristino predefiniti

Le scansioni automatiche coprono tutti gli asset, seguono gli SLA di rimedio predefiniti e tutte le vulnerabilità critiche (CVE 8 o superiori) vengono rimediate in 48 ore o meno dalla pubblicazione da parte del fornitore di software o hardware.

4.2.2 Come ottenete le informazioni sulle vulnerabilità? Selezionare tutte le opzioni applicabili.

- ✓ Vengono ottenuti allarmi sulle vulnerabilità
- ☐ Gli avvisi di vulnerabilità includono notifiche fuori banda (out of band)
- ✓ Gli avvisi di vulnerabilità sono correlati all'ambiente dell'organizzazione per classificare la priorità delle vulnerabilità.
- ☐ Le fonti esterne per le vulnerabilità sono sottoposte ad audit per verificarne l'efficacia almeno una volta all'anno.
- ✓ Vengono utilizzate informazioni generiche sulle minacce (ad esempio, che gli attori delle minacce stanno sfruttando una determinata vulnerabilità; questo include strumenti come il Known Exploited Vulnerability Catalog della CISA).
- ☐ Vengono utilizzate informazioni sulle minacce specifiche per l'organizzazione (comprese le informazioni che gli attori delle minacce potrebbero prendere di mira il Richiedente in modo specifico attraverso lo sfruttamento di una determinata vulnerabilità, o dati provenienti dall'ambiente dell'organizzazione che indicano dove si concentrano gli attori delle minacce).
- ☐ Nessuno dei precedenti

4.2.3 Qual è il tempo obiettivo dell'organizzazione per il dispiegamento di patch 'critiche' – CVE 8 o superiore?

Non esiste una politica definita per quando devono essere distribuite le patch.

Entro 24 ore.

- 24-72 ore.

3-7 giorni

>7 giorni.

4.2.4 Qual è la conformità dell'organizzazione ai propri standard per la distribuzione delle patch critiche?

L'organizzazione non tiene traccia di questa metrica/non lo sa

- >95%
- 90-95%
- 80-89%
- <80%

Asset Inventory

4.3.1 Conservate un inventario dei beni hardware (AssetDeviceManagerSystem / Asset Inventory)?

Controllo non implementato

- Esiste un sistema software di inventario dei beni, ma copre solo alcuni asset
- Esiste un sistema software di inventario dei beni, e copre tutti gli asset

Esiste un meccanismo di inventario automatico degli asset, che copre tutti gli asset e viene aggiornato almeno annualmente.

4.3.2 Conservate un inventario dei beni del software?

Controllo non implementato

- Esiste un sistema software di inventario dei beni, ma copre solo alcuni asset

Esiste un sistema software di inventario dei beni, e copre tutti gli asset

Esiste un meccanismo di inventario automatico degli asset, che copre tutti gli asset e viene aggiornato almeno semestralmente.

4.3.3 Gestite tool automatici di scansione e/o identificazione?

- Controllo non implementato

Gli strumenti di scansione di rilevamento vengono utilizzati per rilevare i dispositivi non autorizzati sulla rete almeno settimanalmente

Gli strumenti di scansione di rilevamento sono utilizzati per rilevare i dispositivi non autorizzati sulla rete almeno quotidianamente.

Gli strumenti di scansione di rilevamento vengono utilizzati per aggiornare l'inventario delle risorse e per rilevare e rimuovere tutti i dispositivi non autorizzati presenti in rete almeno ogni giorno.

4.3.4 Per quanto riguarda la gestione degli "Asset critici" da parte dell'organizzazione, selezionare tutte le opzioni applicabili.

- ☒ L'organizzazione dispone di un inventario dei dati memorizzati - che include il proprietario dei dati, l'asset su cui sono memorizzati, la sensibilità, i limiti di conservazione e i requisiti di smaltimento - per almeno tutti i dati sensibili e lo aggiorna almeno annualmente.
- ☐ L'organizzazione ha definito e documentato gli "asset critici".
- ☐ L'organizzazione ha un processo per identificare attivamente gli "asset critici" e aggiorna l'inventario degli "asset critici" almeno trimestralmente.
- ☐ L'organizzazione stabilisce la priorità degli "Asset critici" in base all'importanza per le operazioni aziendali.
- ☐ Nessuno dei precedenti

Secure Configuration

4.4.1 Stabilire configurazioni standard di sicurezza dei vostri endpoint, ad esempio disabilitando l'esecuzione di codice Java basato su Internet, macro Microsoft Office non attendibili e funzioni di visualizzazione PDF e browser Web non necessarie/non desiderate?

- Controllo non implementato

Vengono stabilite configurazioni standard sicure su alcuni endpoint

Vengono stabilite configurazioni standard sicure su tutti gli endpoint

Vengono stabilite configurazioni standard sicure su tutti gli endpoint e le configurazioni vengono aggiornate sulla base di minacce emergenti o eventi identificati

Logging & Monitoring

4.5.1 I dati di log della sicurezza e dei sistemi sono conservati e monitorati?

Controllo non implementato

- I log vengono conservati e monitorati per alcuni sistemi

I log vengono conservati e monitorati per tutti i sistemi

I log vengono conservati e monitorati per tutti i sistemi per un minimo di 3 mesi

4.5.2 Il vostro processo di registrazione dei Log include quanto segue? Selezionare tutte le voci applicabili.

- ☒ I log vengono abilitati su device locali
- ☐ I log vengono sincronizzati su fonti multiple

- ✓ I log vengono inviati in un sistema di gestione degli eventi e delle informazioni di sicurezza centrali (SIEM)
- ✓ I log vengono riesaminati regolarmente per eventi anomali
- ✓ Il SIEM acquisisce la fonte (firewall, IPS, VPN, etc.)
- ✓ Il SIEM cattura le categorie (attività dell'utente, proxy, etc.)
- ✓ Il SIEM cattura il tipo di informazione (IP, nome, etc.)
- ✓ Il SIEM cattura il caso d'uso (autenticazione, attività sospetta in ingresso, sito web malevolo)
- ✓ I log di sicurezza di tutti i controller di dominio vengono inseriti nel SIEM per l'analisi.
- ✓ I risultati del SIEM vengono esaminati almeno ogni 24 ore da un membro del team IT o di sicurezza informatica.
- ✓ Il monitoraggio della sicurezza è condotto 24 ore su 24, 7 giorni su 7 da un servizio SOC interno o di terze parti.
- ☐ Nessuno dei precedenti

4.5.3 Il vostro processo di monitoraggio della sicurezza include quanto segue? Selezionare tutte le voci applicabili.

- ☐ Il monitoraggio innesca gli allarmi basati sugli Indicatori di Comando e Controllo di compromissione (IOC)
- ☐ Il gruppo di monitoraggio esamina regolarmente le fonti di informazioni sulle minacce per avere gli IOC aggiornati
- ✓ I casi d'uso di monitoraggio vengono regolati in base agli eventi accaduti
- ✓ Il team di monitoraggio indaga sugli eventi di sicurezza segnalati
- ☐ Nessuno dei precedenti

4.5.4 Per quanto riguarda le capacità di monitoraggio della sicurezza e della rete dell'organizzazione, selezionare tutte le opzioni applicabili:

- ✓ L'organizzazione monitora il traffico di rete per rilevare trasferimenti di dati anomali e potenzialmente sospetti.
- ✓ L'organizzazione monitora i problemi di prestazioni e di capacità di archiviazione su tutti i server (ad esempio, utilizzo elevato della memoria o del processore o assenza di spazio libero su disco).
- ☐ L'organizzazione dispone di strumenti per monitorare la perdita di dati (DLP) e sono in modalità di blocco.
- ✓ L'organizzazione utilizza parti esterne per convalidare gli strumenti di monitoraggio della rete e della sicurezza.
- ☐ L'organizzazione dispone di firewall di rete e basati su host che disabilitano le connessioni in entrata per impostazione predefinita.
- ☐ L'organizzazione dispone di un sistema di rilevamento e risposta di rete (NDR-Network Detection and Response).
- ✓ L'organizzazione dispone di una soluzione di isolamento e contenimento delle applicazioni.
- ☐ Nessuno dei precedenti

4.5.5 Quale percentuale di “asset critici” dell'organizzazione viene registrata e inoltrata a una soluzione SIEM?

- ☐ 0-30%
- ☐ 31-50%
- ☐ 51-70%
- ☒ >= 71%
- ☐ Non so

4.5.6 Per quanto riguarda il monitoraggio degli “asset critici” da parte dell'organizzazione, selezionare tutte le opzioni applicabili:

- ☐ L'organizzazione dispone di una funzione interna e/o di un Managed Security Service Provider (“MSSP”) in outsourcing incaricato di monitorare gli avvisi di sicurezza, compresi gli avvisi su “asset critici” (un “Security Operations Center” o “SOC”).
- ☐ Al SOC/MSSP dell'organizzazione viene fornito un elenco aggiornato di “asset critici” con cadenza almeno trimestrale.
- ☐ Il SOC/MSSP dell'organizzazione utilizza una soluzione di monitoraggio delle informazioni e degli eventi di sicurezza (SIEM) per automatizzare la raccolta dei log dagli “asset critici”.
- ✓ Nessuno dei precedenti/Non so.

4.5.7 Se l'organizzazione dispone di un SOC, quest'ultimo ha l'autorità e la capacità di porre rimedio agli eventi di sicurezza (ad esempio, isolando e contenendo gli endpoint da remoto)?

- Sì
- No

4.5.8 Vengono registrati e monitorati i seguenti aspetti relativi alle attività degli amministratori degli utenti? Selezionare tutte le opzioni applicabili.

- ✓ Fonte di registro (log): firewall, IPS, VPN, etc.
- ✓ Categoria di registro (log): Attività dell'Utente, proxy, etc.
- [] Tipologia di informazioni (IP, nome, etc.)
- [] Caso d'uso (autenticazione, attività sospetta in ingresso, sito web malevolo)
- ✓ La registrazione delle attività da amministratore include AD, device di rete, VPN
- [] Modifiche ai gruppi amministratori, incluse aggiunte, modifiche, cancellazioni, accessi (login) falliti
- [] Nessuno dei precedenti

4.5.9 Monitorate attività inusuali/atipiche nelle seguenti tipologie di account e gruppi? Selezionare tutte le voci applicabili.

- ✓ Account amministrativi (sistema e applicazione)
- [] Account di servizio (monitoraggio per accesso interattivo)
- ✓ Account di alto profilo (dirigenziali)
- [] Gruppi Sensibili (Amministratori di Dominio, Amministratori di Schema, terze parti preposte alla sicurezza, etc.)
- [] Nessuno dei precedenti

4.5.10 Per quanto riguarda le capacità dell'organizzazione di monitorare i comportamenti a rischio e gli insider malintenzionati, selezionare tutte le opzioni applicabili:

- [] L'organizzazione dispone di un programma contro le minacce interne
- ✓ L'organizzazione monitora i casi in cui un utente o un account di amministratore imposta una password non sicura
- ✓ L'organizzazione controlla se gli account privilegiati accedono a siti web e servizi non autorizzati.
- ✓ L'organizzazione monitora gli accessi remoti non autorizzati alle "risorse critiche".
- ✓ L'organizzazione monitora sia gli account utente che quelli di amministratore per la comunicazione con siti web, indirizzi IP e altre risorse di gruppi di minacce noti.
- [] Nessuno dei precedenti

Network Security

Network Environment

5.1.1 I dispositivi di rete sono configurati con quanto segue? Selezionare tutte le voci applicabili.

- [] I dispositivi di rete vengono attivati utilizzando configurazioni standard autorizzate
- [] Le modifiche ai dispositivi di rete o alle configurazioni vengono gestite tramite un processo standard di approvazione secondo criteri di business
- [] Le richieste di modifiche alle configurazioni dei dispositivi di rete sono negate per qualsiasi esposizione ad alto rischio
- [] L'accesso amministrativo ai dispositivi di rete viene limitato in base a criteri di "need to know" (strettamente legato alla specifica necessità di accesso all'informazione)
- ✓ Nessuno dei precedenti

5.1.2 Disponete di strumenti di difesa del perimetro di rete che includono firewall, IPS, filtraggio web e rilevamento malware? Selezionare tutte le opzioni applicabili.

- ✓ I firewall coprono tutti i gateway e i breakout di Internet.
- [] Funzionalità di rilevamento e prevenzione delle intrusioni distribuite su tutti i gateway Internet e i breakout Internet.
- [] Le funzionalità di rilevamento del malware coprono tutti i gateway Internet e i breakout.
- [] Il filtraggio del Web copre tutti i gateway Internet e i breakout.

- ☐ Il traffico web viene proxato verso i siti web consentiti e i siti web sconosciuti vengono bloccati.
- ✓ Comunicazione negata su porte TCP/UDP non autorizzate.
- ☐ L'organizzazione dispone di un Web Application Firewall (WAF) davanti a tutte le applicazioni rivolte all'esterno ed è in modalità di blocco.
- ✓ Le risorse dell'organizzazione esposte all'esterno sono segmentate all'interno di una zona demilitarizzata (DMZ) e la DMZ non è direttamente instradabile verso la rete aziendale. Gli utenti che necessitano di accedere ai servizi della DMZ sono instradati verso Internet.
- ☐ Nessuno dei precedenti

5.1.3 Gli ambienti di rete sono logicamente separati per garantire protezione e isolamento dei sistemi critici e dei dati?

Controllo non implementato

Le reti sono fisicamente o logicamente separate per garantire la protezione e l'isolamento di alcuni sistemi e dati critici

- Le reti sono fisicamente o logicamente separate per garantire la protezione e l'isolamento di tutti i sistemi e i dati critici.

Gli ambienti di rete sono fisicamente o logicamente separati per garantire la protezione e l'isolamento di tutti i dati sensibili e la segmentazione viene rivalutata su base annua.

5.1.4 Quale percentuale dell'azienda dell'organizzazione è coperta da scansioni programmate delle vulnerabilità? 80

5.1.5 Con quale frequenza vengono effettuate le scansioni delle vulnerabilità esterne? 1 volta all'anno

5.1.6 Con quale frequenza vengono effettuate le scansioni delle vulnerabilità interne? 1 volta all'anno

5.1.7 Ulteriori commenti sulle scansioni di vulnerabilità:

5.1.8 Per quanto riguarda il modo in cui l'organizzazione convalida l'efficienza e l'efficacia dei controlli di sicurezza, selezionare tutte le opzioni applicabili:

- ✓ L'organizzazione mantiene un inventario delle risorse esposte all'esterno.
- ✓ L'organizzazione conduce almeno una volta all'anno un test di penetrazione per valutare la sicurezza dei sistemi rivolti all'esterno.
- ☐ L'organizzazione dispone di un "red team" per testare i controlli di sicurezza o, almeno una volta all'anno, si avvale di esperti per eseguire un test di penetrazione incentrato sui sistemi interni.
- ☐ L'organizzazione esegue almeno mensilmente una scansione delle risorse esposte all'esterno alla ricerca di vulnerabilità.
- ✓ L'organizzazione utilizza un servizio esterno per monitorare la propria superficie di attacco (sistemi esterni/interni).
- ☐ L'organizzazione utilizza un software di simulazione di violazione e attacco (BAS) per verificare l'efficacia dei controlli di sicurezza.
- ☐ L'organizzazione ha ingaggiato una parte esterna per simulare gli attori delle minacce e testare i controlli di sicurezza nell'ultimo anno.
- ☐ L'organizzazione ha condotto una caccia alle minacce di rete negli ultimi 12 mesi.
- ☐ L'organizzazione ha condotto un Threat Hunt su servizi cloud (Office 365, Amazon Web Services, ecc.) negli ultimi 12 mesi.
- ☐ Nessuno dei precedenti

Wireless

5.2.1 Proteggete i vostri dispositivi di rete wireless utilizzando i seguenti controlli? Selezionare tutte le voci applicabili.

- ☐ Tutti i dispositivi di rete wireless non autorizzati/punti di accesso vengono rilevati e rimossi
- ☐ Le password e gli SSID predefiniti (di default) vengono modificati su tutti i dispositivi wireless
- ✓ L'accesso è limitato per tutti i dispositivi wireless
- ✓ Viene utilizzato lo standard minimo di crittografia WPA
- ☐ Il firewall di rilevamento delle intrusioni basato sull'host viene installato su tutti i dispositivi
- ☐ L'accesso wireless viene disabilitato su tutti i dispositivi che non lo necessitano per uno scopo strettamente di business
- ✓ Viene utilizzata una rete wireless separata per i dispositivi personali o non affidabili
- ☐ Nessuno dei precedenti

Network Penetration Testing

5.3.1 Vi siete affidati a terzi per i test di penetrazione esterna sulla vostra rete?

Non viene condotto alcun test di penetrazione

I test di penetrazione vengono effettuati solo dal team di test interno

- Una terza parte viene utilizzata per test di penetrazione esterna sulla nostra rete occasionalmente e per casi specifici

Una terza parte viene utilizzata per test di penetrazione esterna sulla nostra rete almeno una volta l'anno e le vulnerabilità critiche identificate sono mitigate o risolte entro un periodo di due settimane

Network Capacity

5.4.1 Il sistema gestisce la capacità in eccesso, la larghezza di banda o altre ridondanze per limitare gli effetti di attacchi DDoS effettuati tramite flooding di dati?

- Controllo non implementato

La rete gestisce capacità in eccesso, larghezza di banda o ridondanza, tuttavia copre piccole aree di attività dell'azienda o non copre adeguatamente aree critiche

La rete gestisce capacità in eccesso, larghezza di banda o ridondanza per limitare il rischio di indisponibilità del servizio per le attività di business più rilevanti

La rete gestisce capacità in eccesso, larghezza di banda o ridondanza per limitare il rischio di indisponibilità del servizio per tutte le attività di business

Physical Security

Physical Access

6.1.1 Limitate l'accesso esclusivamente al vostro personale e ai fornitori, agenti o visitatori autorizzati?

Controllo non implementato

Viene limitato l'accesso ad alcuni luoghi dell'azienda esclusivamente al nostro personale e ai fornitori, agenti o visitatori autorizzati

- Viene limitato l'accesso a tutti i luoghi dell'azienda esclusivamente al nostro personale e ai fornitori, agenti o visitatori autorizzati

Physical Penetration Testing

6.2.1 Vi affidate a terzi per i test di penetrazione esterna sulle vostre proprietà fisiche?

- Non viene condotto alcun test di penetrazione

I test di penetrazione vengono effettuati solo dal team di test interno

Una terza parte viene utilizzata per test di penetrazione esterna su luoghi dell'azienda critici, su base occasionale ed esigenze specifiche

Una terza parte viene utilizzata per test di penetrazione esterna su luoghi dell'azienda critici almeno una volta l'anno

Tampering & Alteration

6.3.1 Eseguite ispezioni per la manomissione fisica o l'alterazione di componenti hardware all'interno del sistema?

- Controllo non implementato
Vengono eseguite ispezioni per manomissioni fisiche su alcuni sistemi
Vengono eseguite ispezioni per manomissioni fisiche su tutti i sistemi
Vengono eseguite ispezioni per manomissioni fisiche su tutti i sistemi e più frequentemente in occasione di eventi significativi (ad es. manutenzione ordinaria)

Environmental

6.4.1 Le vostre strutture sono dotate di sistemi di aria condizionata, rilevamento di acqua, rilevamento di umidità, rilevamento di calore/fumo, pavimenti sopraelevati e sistemi antincendio per proteggere le apparecchiature informatiche?

- Controllo non implementato
Sono predisposte alcune protezioni, tuttavia coprono piccole aree dell'azienda o non coprono adeguatamente tutte le aree critiche
Le strutture sono configurate con la maggior parte dei sistemi elencati per proteggere le apparecchiature informatiche
- Le strutture sono configurate con tutti i sistemi elencati per proteggere le apparecchiature informatiche

6.4.2 Le vostre strutture sono dotate di un sistema di alimentazione elettrica ininterrotta per almeno 48 ore (sistema di continuità)?

- Controllo non implementato
Alcune strutture hanno un alimentatore di energia di continuità
- Le strutture chiave critiche (ad es. data center) hanno un alimentatore di energia di continuità
Tutte le strutture hanno un alimentatore di energia di continuità per almeno 48 ore

Application Security

Training

7.1.1 Avete una formazione formalizzata sulla sicurezza per gli sviluppatori?

- Controllo non implementato
La formazione sulla sicurezza è obbligatoria per alcuni sviluppatori
La formazione sulla sicurezza è obbligatoria per tutti gli sviluppatori con cadenza almeno annuale
La formazione sulla sicurezza è obbligatoria per tutti gli sviluppatori con cadenza almeno annuale e include aggiornamenti periodici per adeguarsi alle minacce emergenti

Secure Development

7.2.1 Impiegate firewall su applicazioni e bloccate accessi non autorizzati ai sistemi critici?

- Controllo non implementato
- Vengono impiegati firewall su alcune applicazioni
Vengono impiegati firewall su tutte le applicazioni, ma non bloccano sempre gli accessi non autorizzati
Vengono impiegati firewall su tutte le applicazioni e bloccano gli accessi non autorizzati

7.2.2 Le vostre prassi di sviluppo software sicuro includono i seguenti controlli? Selezionare tutte le voci applicabili.

- ☐ Convalida il controllo esplicito degli errori e l'accuratezza dei dati inseriti (ad esempio dimensioni, tipo di dati, intervalli accettabili, formati, ecc.)
- ☐ Verifica di autenticazione o autorizzazione compromessa / invalida
- ☐ Verifica su algoritmi di cifratura standard
- ☐ Garanzia che le versioni software siano rinforzate e supportate
- ☐ Utilizzo esclusivamente di fornitori di fiducia per l'impiego di software di terze parti
- ☐ Utilizzo di tool di verifica dell'integrità per rilevare modifiche di configurazioni di sicurezza non autorizzate e rilevanti per il software e le informazioni
- ☒ Nessuno dei precedenti

7.2.3 Il vostro ciclo di vita della sviluppo del software richiede le seguenti attività? Selezionare tutte le voci applicabili.

- ☒ Separazione degli ambienti di sviluppo dagli ambienti di produzione
- ☐ Separazione dei compiti tra team di sviluppo e team in produzione
- ☐ Offuscamento dei dati durante i test e distruzione dei dati al completamento dei test
- ☐ Nessuno dei precedenti

7.2.4 Eseguite i seguenti tipi di test di penetrazione delle applicazioni? Selezionare tutte le voci applicabili.

- ☐ Scansione delle applicazioni web
- ☐ Test di penetrazione delle applicazioni mobili
- ☐ Analisi del codice dinamico (es. DAST, Black-Box, Gray-Box testing)
- ☐ Analisi del codice statico (es. SAST, White-Box testing)
- ☐ Analisi del codice interattivo (es. IAST o RIA)
- ☐ Analisi della Composizione del Software
- ☐ Modellizzazione delle Minacce Applicative (Application Threat Modelling)
- ☐ Protezione del Software dell'Applicazione a Runtime (ad es. RASP)
- ☒ Nessuno dei precedenti

Software Management

7.3.1 In che modo controllate l'esecuzione di un software non autorizzato?

Controllo non implementato

- L'inventario delle applicazioni viene mantenuto manualmente utilizzando un elenco di software approvato

L'inventario delle applicazioni viene mantenuto e qualsiasi software non autorizzato identificato viene rimosso in modo tempestivo

La tecnologia White-listing è implementata su tutti i dispositivi per controllare l'esecuzione del software ed è aggiornata almeno due volte all'anno.

7.3.2 La vostra tecnologia di autorizzazione ("white-listing") delle applicazioni include quanto segue?

Il white-listing delle applicazioni attualmente non è implementato

- Il white-listing delle applicazioni include i file eseguibili (.exe)

Il white-listing delle applicazioni include i file eseguibili e le librerie di codici (.dll, .ocx)

Il white-listing delle applicazioni include i file eseguibili, le librerie di codici e gli script (macros, .ps1)

7.3.3 Come gestite il software a fine vita o a fine supporto (End of Life o End of Support? Selezionare tutte le opzioni applicabili.

- ☐ L'organizzazione non dispone di software a fine vita (EoL) o a fine supporto (EoS)
- ☐ L'organizzazione dispone di un database aggiornato per la gestione della configurazione (CMDB).
- ☐ Il software a fine vita (EoL) o a fine supporto (EoS) dell'organizzazione è segregato dal resto della rete.
- ☐ L'organizzazione dispone di un processo di dismissione del software o delle applicazioni inutilizzate (SMBv1, ecc.).

✓ L'organizzazione acquista supporto aggiuntivo per il software a fine vita, se disponibile.

[] Nessuno dei precedenti

7.3.4 Quali piattaforme end of life (EoL) sono in uso? (ad esempio Windows 7, XP, 2008) windows 2008 e alcune postazione PC windows 7

- Commenti: è costante l'attività di aggiornamento delle piattaforme

7.3.5 Quanti server/postazioni di lavoro operano su piattaforme a fine vita? 20

7.3.6 Queste macchine gestiscono informazioni sensibili o supportano funzioni aziendali critiche?

Sì

• No

7.3.7 Qual è la tempistica (mese/anno) per la dismissione di questi sistemi? 12/2026

Third Party

Third-Party Contracts

8.1.1 Per contratto richiedete a terzi di allinearsi ai servizi predefiniti e ai Service Level Agreement (SLA) per il Cyber?

Le terze parti non sono contrattualmente obbligate ad allinearsi con servizi e SLA predefiniti per il Cyber

• Alcune terze parti sono contrattualmente obbligate ad allinearsi con servizi e SLA predefiniti per il Cyber

Tutte le terze parti sono contrattualmente obbligate ad allinearsi con servizi e SLA predefiniti per il Cyber

Tutte le terze parti sono contrattualmente obbligate ad allinearsi con servizi e SLA predefiniti per il Cyber che vengono aggiornate in base al cambiamento dei servizi

8.1.2 Richiedete contrattualmente alle terze parti di avere permanentemente la copertura di un'assicurazione o di altra forma di indennizzo, per eventuali perdite causate dalla terza parte stessa?

Le terze parti non sono contrattualmente obbligate ad avere permanentemente la copertura di un'assicurazione o di altra forma di indennizzo, per eventuali perdite

Alcune delle terze parti sono contrattualmente obbligate ad avere permanentemente la copertura di un'assicurazione o di altra forma di indennizzo, per eventuali perdite

Tutte le terze parti sono contrattualmente obbligate ad avere permanentemente la copertura di un'assicurazione o di altra forma di indennizzo, per eventuali perdite

• Tutte le terze parti sono contrattualmente obbligate ad avere permanentemente la copertura di un'assicurazione o di altra forma di indennizzo, per eventuali perdite, le cui clausole vengono aggiornate in base al cambiamento dei servizi

Due Diligence

8.2.1 Svolgete una due diligence sulle terze parti affinché siano allineate alle vostre politiche aziendali interne e/o alle best practice del settore?

• Questo processo/procedura non è attualmente impiegato in azienda

Alcune terze parti vengono valutate

Tutte le terze parti vengono valutate

Tutte le terze parti vengono valutate e rivalutate in funzione di eventuali cambiamenti degli accordi di servizio

8.2.2 Eseguite verifiche di business continuity e disaster recovery sui vostri fornitori?

- Controllo non implementato

Alcune terze parti vengono incluse in audit di business continuity e di disaster recovery

Tutte le terze parti vengono incluse in audit di business continuity e di disaster recovery

Tutte le terze parti vengono incluse in audit di business continuity e di disaster recovery, incluse le revisioni successive a cambiamenti organizzativi

8.2.3 Eseguite una valutazione sull'impatto commerciale dei rischi informatici associati a terze parti?

- Controllo non implementato

Le valutazioni vengono eseguite tramite un approccio informale o a sensazione

Le valutazioni vengono eseguite tramite un approccio formalizzato

Le valutazioni vengono eseguite tramite un'analisi formalizzata utilizzando la modellizzazione dei potenziali impatti finanziari

8.2.4 Utilizzate soglie predefinite e processi di escalation che facilitino la decisione di applicare strategie di cybersecurity nei confronti di terze parti specifiche?

- Controllo non implementato

Vengono utilizzate soglie e processi di escalation su base occasionale e specifica

Una metodologia formale e un canale di segnalazione aiutano a determinare strategie di cybersecurity appropriate per terze parti

Un approccio formale, con l'impiego di metriche multiple, strategie di gestione coerenti, e il coinvolgimento del senior management aiutano a determinare strategie di cybersecurity appropriate per terze parti

Third-Party Inventory

8.3.1 Per quanto riguarda il ruolo di terze parti o di Managed Service Provider (MSP) nella rete dell'organizzazione, compreso l'accesso remoto a risorse quali cloud e VPN, selezionare tutte le opzioni applicabili:

- ☐ L'organizzazione utilizza un MSP per l'amministrazione di "asset critici".
- ☐ L'organizzazione utilizza un MSP per le operazioni di sicurezza
- ☐ L'organizzazione utilizza un MSP per il backup e il ripristino dei dati.
- ☐ L'organizzazione utilizza un MSP per la trasformazione in cloud
- ☐ L'organizzazione utilizza un MSP per lo sviluppo del software
- ☐ L'organizzazione fornisce a terzi un accesso persistente ("always on") alle risorse aziendali (l'accesso non richiede l'autorizzazione dell'organizzazione).
- ✓ Nessuno dei precedenti

8.3.2 Conservate un inventario dei fornitori chiave con accesso ai sistemi o dati?

Controllo non implementato

Esiste un elenco dei fornitori, ma ne include solo alcuni

Esiste un elenco completo dei fornitori

- Esiste un elenco completo dei fornitori, che viene aggiornato in base ai cambiamenti organizzativi

Business Resilience

Business Continuity/DR

9.1.1 Avete un piano di continuità operativa (BCP) e un piano tecnico di disaster recovery (DR)?

- Il processo non è attualmente implementato all'interno dell'azienda

Abbiamo piani di Business Continuity e Disaster Recovery per alcune aree di business

Abbiamo piani di Business Continuity e Disaster Recovery tecnico per tutte le aree di business

Abbiamo piani di Business Continuity e Disaster Recovery tecnico per tutte le aree di business, che vengono testati ogni anno

9.1.2 Il vostro piano BCP/DR consente il ripristino a partire dai seguenti eventi? Selezionare tutte le voci applicabili.

- ☐ Guasto/indisponibilità di una tecnologia o software critico
- ☐ Guasto/indisponibilità di un fornitore di tecnologie critiche o di una utility
- ☐ Perdita o danneggiamento di qualsiasi informazione critica
- ☐ Divulgazione di informazioni criticamente sensibili
- ☒ Nessuno dei precedenti

9.1.3 I vostri piani BCP/ DR tengono conto dei seguenti tipi di impatto finanziario tangibile? Selezionare tutte le voci applicabili.

- ☐ Costo-opportunità
- ☐ Aumento del costo del lavoro e delle spese
- ☐ Riduzione del valore dei ricavi (o equivalente)
- ☐ Inefficienza e redditività
- ☐ Sostituzione di beni non assicurati
- ☐ Costo del denaro e sostenibilità finanziaria
- ☒ Nessuno dei precedenti

9.1.4 Il vostro programma di esercitazioni BCP/DR include quanto segue? Selezionare tutte le voci applicabili.

- ☐ Le esercitazioni sono condotte e aggiornate su base regolare e pianificata
- ☐ Le esercitazioni coprono tutte le operazioni necessarie per ripristinare il business
- ☐ Ogni esercitazione è seguita da un report con indicazioni per il miglioramento
- ☐ Tutto il personale chiave partecipa alle esercitazioni sul piano BCP/DR
- ☐ Il piano di esercitazioni BCP/DR include il ripristino dei sistemi critici
- ☒ Nessuno dei precedenti

Incident Response

9.2.1 Avete in atto un piano di risposta agli incidenti di cybersecurity affronti i seguenti aspetti? Selezionare tutte le voci applicabili.

- ☒ Identificazione di un incidente di cybersecurity
- ☒ Investigazione della situazione (incluso il triage)
- ☐ Attuazione delle azioni appropriate (ad es. contenendo l'incidente e debellando la sua origine)
- ☒ Segnalazione agli stakeholder interessati
- ☐ Recupero da un incidente di cybersecurity
- ☐ Nessuno dei precedenti

9.2.2 Con quale frequenza rivedete e aggiornate i piani di risposta agli incidenti?

- ☐ I piani di risposta agli incidenti non vengono rivisti nè aggiornati
- ☐ I piani di risposta agli incidenti vengono rivisti e aggiornati occasionalmente
- ☒ I piani di risposta agli incidenti vengono rivisti e aggiornati annualmente
- ☐ I piani di risposta agli incidenti vengono rivisti e aggiornati trimestralmente

9.2.3 Eseguite esercitazioni simulate con i seguenti requisiti? Selezionare tutte le voci applicabili.

- ☐ Le esercitazioni simulate sono basate su rischi e minacce emergenti
- ☐ Le esercitazioni simulate coinvolgono gli stakeholder elencati in un piano di risposta agli incidenti
- ☒ Le esercitazioni simulate coinvolgono il senior management
- ☒ Le lezioni apprese/azioni di miglioramento sono documentate dopo le esercitazioni simulate
- ☐ Nessuno dei precedenti

9.2.4 Avete mai collaborato con uno dei seguenti fornitori di sicurezza per la risposta ad incidenti? Selezionare tutte le voci applicabili.

- ☐ Coach per la gestione della violazione
- ☒ Consulente legale
- ☐ Relazioni pubbliche
- ☐ Forense
- ☐ Scoperta elettronica
- ☐ Notifica e monitoraggio
- ☐ Prevenzione della violazione
- ☐ Nessuno dei precedenti

9.2.5 Qual è il tempo medio dell'organizzazione per il triage e il contenimento degli incidenti di sicurezza delle postazioni di lavoro?

L'organizzazione non tiene traccia di questa metrica/non lo sa

< 30 minuti

- Da 30 minuti a 2 ore

Da 2 a 8 ore

Da 8 ore a 3 giorni

> 3 giorni

9.2.6 Avete definito gli obiettivi di tempo di ripristino (RTO) commisurati alle vostre esigenze di continuità operativa?

- Sì
- No

9.2.7 Se sì, qual è l'RTO per gli asset più critici dell'organizzazione?

< 5 ore.

5-12 ore.

- 12-24 ore.

1-7 giorni.

> 7 giorni.

- Commenti: RTO minore

9.2.8 Se no, qual è la tempistica per l'implementazione da parte dell'organizzazione?

9.2.9 L'organizzazione testa la propria capacità di ripristinare diversi "asset critici" in conformità con l'obiettivo di tempo di ripristino (RTO) con cadenza almeno trimestrale?

Sì

- No

9.2.10 Commento aggiuntivo sulla valutazione e sugli obiettivi del recupero:

Backup

9.3.1 Il vostro processo di backup copre quanto segue? Selezionare tutte le voci applicabili.

- ✓ Applicazioni
- ✓ Database
- ☐ Endpoint
- ✓ Unità di Rete (inclusi quelli utilizzati dagli individui)
- ✓ Strumenti di collaborazione (es. SharePoint)
- ✓ Configurazioni di Sistema
- ☐ Sistemi correlati a OT (se applicabili)
- ☐ Nessuno dei precedenti

9.3.2 I backup sono soggetti alle seguenti misure, selezionare tutte quelle applicabili:

- ☐ Autenticazione Multifattore
- ☐ Segmentazione
- ✓ Cifratura
- ✓ Immutabile
- ✓ Scansione di virus/malware
- ✓ Le credenziali di backup sono uniche e conservate separatamente dalle altre credenziali
- ✓ I sistemi di backup critici sono testati
- ✓ Il processo di backup è condotto tramite una soluzione automatizzata
- ✓ La frequenza dei backup è definita in base alla criticità aziendale
- ☐ Nessuno dei precedenti

9.3.3 Utilizzate fornitori di servizi cloud per alcuno dei seguenti servizi come parte della vostra strategia di backup per accelerare il recupero di eventuali perdite di dati? Selezionare tutte le voci applicabili.

- ☐ La soluzione cloud offre hardware e firmware di riserva
- ☐ La soluzione cloud consente rapide ricostruzioni di O/S, software e applicazioni
- ☐ La soluzione cloud offre funzionalità di ripristino di dispositivi mobili
- ☐ La soluzione cloud offre e-mail basate su cloud
- ✓ Nessuno dei precedenti

9.3.4 Con quale frequenza viene eseguito il backup delle informazioni critiche? Seleziona tutte le risposte applicabili.

- ✓ Quotidianamente
- ☐ Settimanalmente
- ☐ Mensilmente
- ☐ Trimestralmente
- ☐ Semestralmente
- ☐ Annualmente
- ☐ Nessuno dei precedenti

9.3.5 Dove vengono archiviati i backup? Selezionare tutte le opzioni.

- ☐ Cloud - servizio di sincronizzazione (es. DropBox, OneDrive, SharePoint, Google Drive)
- ☐ Cloud - servizio non sincronizzato
- ✓ In sede
- ✓ Archiviazione offline
- ✓ Archiviazione fuori sede
- ✓ Data center secondario
- ☐ Nessuno dei precedenti

9.3.6 L'organizzazione è in grado di testare l'integrità dei backup prima del ripristino per essere certa che siano privi di malware?

- Sì
- No

9.3.7 Si prega di fornire ulteriori commenti sui backup. In particolare, si delinei il programma di rotazione dei backup dell'organizzazione.

backup giornalieri on line e riversamenti settimanali su cassette off line (DAT)

Remote Work

Remote Connectivity

10.1.1 Che tipo di dispositivi utilizzano i dipendenti quando lavorano in remoto?

- Dispositivi aziendali preconfigurati con build standard
- Dispositivi aziendali non configurati
- Dispositivi personali dedicati
- BYOD condiviso

10.1.2 Esistono politiche per monitorare e revocare l'accesso remoto?

- Controllo non implementato
- La funzionalità esiste, ma non è monitorata
- Funzionalità reattiva presente
- Funzionalità presente, applicata in modo proattivo e allineata alle politiche aziendali

10.1.3 L'organizzazione consente connessioni esterne alla rete utilizzando uno dei seguenti protocolli Internet? Selezionare tutti quelli che si applicano.

- ☐ Remote Desktop Protocol (RDP)
- ☐ Telnet
- ☐ NetBIOS
- ☐ Blocco dei messaggi del server (SMB)
- ☐ Istanze desktop virtuali (VDI)
- ☒ Nessuno dei precedenti

10.1.4 Se l'organizzazione consente connessioni esterne alla rete tramite RDP o VDI, sono state implementate le seguenti misure? Selezionare tutte le opzioni applicabili.

- ☒ Solo accesso VPN
- ☒ Autenticazione dell'accesso a più fattori
- ☐ Autenticazione a livello di rete abilitata
- ☐ Honeypot RDP
- ☐ Nessuno dei precedenti

Authentication & Identity

10.2.1 In che modo i lavoratori da remoto eseguono l'autenticazione ai sistemi/dati aziendali?

Non applicabile – autenticazione non presente

- Autenticazione di base (nome utente/password) per i sistemi principali
Autenticazione di base per i sistemi principali e autenticazione a più fattori per i sistemi critici
Viene utilizzato il single sign-on per il sistema chiave in aggiunta all'autenticazione a più fattori

10.2.2 Supportate, applicate e abilitate la gestione dei dispositivi mobili?

- Controllo non implementato
MDM implementato sui dispositivi aziendali, BYOD consentito ma non applicato
MDM implementato sui dispositivi aziendali, BYOD non consentito
MDM implementato su tutti i dispositivi collegati

Device Vulnerability & Monitoring

10.3.1 La scansione e la gestione delle vulnerabilità sono abilitate per i dispositivi remoti?

- Controllo non implementato
Controllo implementato per la scansione delle risorse aziendali, ma non dei BYOD
Controllo implementato per tutti i dispositivi collegati, incluse risorse aziendali e BYOD
Controllo presente per tutti i dispositivi collegati con gli aggiornamenti della sicurezza abilitati

10.3.2 Avete un monitoraggio protettivo (ad es. servizi SOC) abilitato per tutte le risorse in remoto?

- Controllo non implementato
Monitoraggio parziale di alcune risorse presente a livello di rete
Monitoraggio reattivo presente per tutti i punti finali utilizzando strumenti avanzati come il rilevamento e la risposta degli endpoint (EDR)
Monitoraggio proattivo presente per tutti gli end-point utilizzando strumenti avanzati (ad es EDR); monitoraggio protettivo e risposta abilitati per la gestione di incidenti quali il controllo dell'accesso alla rete (NAC), la gestione degli accessi privilegiati (PAM), il rilevamento e la risposta gestiti (MDR) e la prevenzione della perdita di dati (DLP)

Remote Business Continuity

10.4.1 Che tipo di sistema di backup viene utilizzato per i dispositivi che si connettono in remoto?

- Non disponibile: il backup non è abilitato per gli utenti remoti
Backup di alcuni dati abilitato, eseguito centralmente quando connesso
Backup di alcuni dati abilitato, eseguito sia localmente sia centralmente
Il backup di tutti i dati è stato abilitato, eseguito localmente e centralmente a intervalli regolari pianificati in linea con le politiche per la sicurezza/i dati

10.4.2 I piani di Business Continuity (BCP) e Disaster Recovery (DR) sono stati valutati, sviluppati e testati per il lavoro remoto su larga scala? Selezionare tutte le risposte pertinenti.

- ☐ L'analisi dell'impatto aziendale prende in considerazione i requisiti delle risorse durante gli accordi di lavoro remoto su larga scala
- ☐ Le strategie e le procedure BCP e DR sono sviluppate per affrontare il lavoro remoto su larga scala
- ☐ Esercitazioni e simulazioni hanno incluso scenari di lavoro remoto su larga scala
- ☒ Nessuno dei precedenti

Remote Security Awareness

10.5.1 Con quale frequenza la formazione su sicurezza e consapevolezza copre i rischi del lavoro da remoto implementati su tutta la base di utenti?

Controllo non implementato

- Annualmente
- Trimestralmente
- Mensilmente

Cyber Crime

Cyber Crime

11.1.1 Tutti i bonifici sono soggetti a un processo in tre fasi (avvio, approvazione e rilascio) da parte di due o più persone autorizzate (es. segregation of duties) ?

- Si
- No
- N/A

11.1.2 È previsto un processo di richiamo o di notifica alternativa (es. chiamata telefonica) per tutti i trasferimenti informatici di fondi?

- Si
- No
- N/A

LA PRESENTE AON CYBER QUOTIENT EVALUATION (AON CYBER EVALUATION) E' INCORPORATA A QUALSIASI APPLICAZIONE PER CYBEREDGE COVERAGE (SM) PRESENTATA DAL RICHIEDENTE. TUTTE LE DICHIARAZIONI E LE GARANZIE RILASCIATE DAL RICHIEDENTE IN RELAZIONE A TALE RICHIESTA DI COPERTURA CIBERNETICA, NONCHE' TUTTE LE NOTE LEGALI, SI APPLICANO ANCHE ALLE INFORMAZIONI FORNITE IN QUESTA VALUTAZIONE CIBERNETICA

Firmato: _____

(Rappresentante debitamente autorizzato da e per conto del richiedente)

Data: _____

Titolo: _____

Organizzazione: _____

© Aon s.p.a. o le sue consociate ("Aon"). Tutti i diritti riservati.