INAPP
ISTITUTO NAZIONALE PER L'ANALISI DELLE POLITICHE PUBBLICHE

ADA.14.01.18 - SVILUPPO DELLA STRATEGIA PER LA SICUREZZA INFORMATICA (D1)

RIEPILOGO SCHEDA DI CASO

RISULTATO ATTESO 1 - Definire e rimodulare la strategie e le politiche aziendali di Information Security, a partire dalla individuazione di standard e requisiti legali di riferimento, curando anche gli aspetti organizzativi relativi alla sua implementazione

CASI ESEMPLIFICATIVI:

Dimensione 1 - Definizione strategia per la Sicurezza Informatica: **5 casi**

Dimensione 2 - Aggiornamento strategia per la Sicurezza Informatica: **5 casi**

RISORSE A SUPPORTO DELLA VALUTAZIONE (RSV)

INAPP
ISTITUTO NAZIONALE PER L'ANALISI DELLE POLITICHE PUBBLICHE

ADA.14.01.18 - SVILUPPO DELLA STRATEGIA PER LA SICUREZZA INFORMATICA (D1)

SCHEDA DI CASO

RISULTATO ATTESO 1 - Definire e rimodulare la strategie e le politiche aziendali di Information Security, a partire dalla individuazione di standard e requisiti legali di riferimento, curando anche gli aspetti organizzativi relativi alla sua implementazione

1 - DEFINIZIONE STRATEGIA PER LA SICUREZZA INFORMATICA

Grado di complessità 2

1.2 SVILUPPO STRATEGIA

Sviluppare la strategia aziendale per la Sicurezza Informatica individuando la visione generale, gli obiettivi, i target e le misure, sulla base delle ricerche e analisi precedentemente condotte in tema di requisiti legali, best practice e posizionamento aziendale

1.2 RISK ANALYSIS

Eseguire un'analisi del rischio che evidenzi, sulla base di una scala di importanza, le minacce e le vulnerabilità dell'Ecosistema legale, normativo e di business (in quest'ultimo caso, individuando l'evento, le probabilità che questo accada, e l'eventuale danno), finalizzata alla formalizzazione di un piano di trattamento del rischio che preveda l'esecuzione di attività rispetto ai pilastri fondamentali della Sicurezza Informatica (People, Process & Technology)

Grado di complessità 1

1.1 INDIVIDUAZIONE REQUISITI LEGALI

Individuare i riferimenti normativi (es. Direttiva NIS e Regolamento Generale sulla Protezione dei Dati) attraverso un'attenta ricerca delle fonti istituzionali

1.1 INDIVIDUAZIONE BEST PRACTICE

Individuare, attraverso un'ampia attività di ricerca, best practice (es. ITIL, COBIT, ecc.) per poter adottare elevati standard in merito alla Sicurezza Informatica all'interno dell'azienda

1.1 BUSINESS ENVIRONMENT ANALYSIS

Analizzare i requisiti di business tipici dell'organizzazione considerata per allineare le strategie, in termini di Sicurezza Informatica, a tali requisiti di business (ISO/IEC 27001, ISO/IEC 20000, ISO 22301, ecc.)

2 - AGGIORNAMENTO STRATEGIA PER LA SICUREZZA INFORMATICA

ADA.14.01.18 - SVILUPPO DELLA STRATEGIA PER LA SICUREZZA INFORMATICA (D1)

Grado di complessità 3

2.3 AGGIORNAMENTO STRATEGIA

Rimodulare la strategia per la Sicurezza Informatica sulla base dei risultati di monitoraggio

2.3 ANALISI DATI

Analizzare dati di security analytics (es. threat detection, riconoscimento di cyber attacchi, ecc.), modificando, in caso di risultati poco soddisfacenti, i tools utilizzati

Grado di complessità 2

2.2 MONITORAGGIO DELL'IMPLEMENTAZIONE DELLA STRATEGIA

Rilevare ed analizzare i dati inerenti all'applicazione della strategia definita, secondo le modalità automatizzate di Information Security Continuous Monitoring (ISCM)

Grado di complessità 1

2.1 MONITORAGGIO EVOLUZIONE NORMATIVA

Tenere traccia dell'evoluzione normativa nazionale ed europea sulla Sicurezza Informatica e, sulla base di ciò, modificare la strategia aziendale

2.1 MONITORAGGIO EVOLUZIONE BEST PRACTICES

Tenere traccia dell'evoluzione delle best practice in merito alla Sicurezza Informatica, ad esempio, attraverso la partecipazione a convegni di disseminazione di informazione organizzati da istituti di ricerca riconosciuti, trasmettendo al team aziendale preposto i risultati presentati in modo da valutare un eventuale aggiornamento della strategia

INAPP
ISTITUTO NAZIONALE PER L'ANALISI DELLE POLITICHE PUBBLICHE

ADA.14.01.18 - SVILUPPO DELLA STRATEGIA PER LA SICUREZZA INFORMATICA (D1)

SCHEDA RISORSE A SUPPORTO DELLA VALUTAZIONE DEL RISULTATO ATTESO 1

RISORSE FISICHE ED INFORMATIVE TIPICHE (IN INPUT E/O PROCESS ALLE ATTIVITÀ)

- Pilastri fondamentali della Sicurezza Informatica (People, Process & Technologies)
- Normative vigenti in Italia (es. Direttiva NIS, Regolamento Generale sulla Protezione dei Dati, ecc.)
- Best practice di Sicurezza Informatica (es. ITIL, COBIT, ecc.)
- Schemi di certificazione (ISO/IEC 27001, ISO/IEC 20000, ISO 22301, ecc.)
- e-Competence Framework relativo alle competenze ICT
- Dati di security analytics
- Corsi e-learning
- Caratteristiche dell'ecosistema legale, normativo e di requisiti di business

TECNICHE TIPICHE DI REALIZZAZIONE/CONDUZIONE DELLE ATTIVITÀ

- Tecniche di analisi dati di security analytics
- Tecniche di conduzione di analisi del rischio
- Tecniche di conduzione di analisi di business environment
- Metodi e tecniche di sviluppo di corsi di formazione online
- Metodi e tecniche di management di organizzazione aziendale

OUTPUT TIPICI DELLE ATTIVITÀ

- Analisi del rischio condotta
- Analisi del business enviornment condotta
- Strategia per la Sicurezza Informatica sviluppata/aggiornata
- Corsi di formazione online erogati
- Team preposto alla Sicurezza Informatica nominato

INDICAZIONI A SUPPORTO DELLA SCELTA DEL METODO VALUTATIVO E DELLA PREDISPOSIZIONE DELLE PROVE

ESTENSIONE SUGGERITA DI VARIETÀ PRESTAZIONALE

1. L'insieme degli ecosistemi legali, normativi e di requisiti di business
2. L'insieme delle normative vigenti in tema di Sicurezza Informatica
3. Un set di casi descritti in termini di requisiti normativi, best practice e posizionamento aziendale”

DISEGNO TIPO DELLA VALUTAZIONE

1. Prova prestazionale: per almeno un ecosistema dato, impostazione/sviluppo simulato di una strategia per la Sicurezza Informatica
2. Colloquio tecnico relativo alle best practice e fondamenti di management di un modello organizzativo non oggetto di prova prestazionale

FONTI

Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione
https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016L1148
Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32016R0679

European e-Competence Framework https://www.ecompetences.eu/
Franchi, A. (2020). Effetti dell'implementazione di sistemi di gestione della sicurezza delle informazioni sulla sicurezza informatica aziendale reale e percepita, Department of Business Administration program at Selinus University

SITOGRAFIA
https://www.iso.org/isoiec-27001-information-security.html
https://www.isaca.org/resources/cobit
https://www.agendadigitale.eu/sicurezza/cyber-security-cosi-impostiamo-la-strategia-corretta-in-azienda/
https://www.cybersecurityframework.it/
https://www.cybersecurity360.it/soluzioni-aziendali/information-security-continuous-monitoring-le-linee-guida/