Punto della situazione

Domande orientative ai fornitori

# Da compilare da parte della divisione IT/OT interna:

|  |  |
| --- | --- |
| Numero del fornitore: |       |
| Interlocutore principale: |       |
| Filiale: |       |
| Attivo nelle filiali: |       |
| Questionario n.: |       |

# Da compilare da parte del partner:

|  |  |
| --- | --- |
| Nome del fornitore: |       |
| Prestazione del fornitore: |       |
| Descrizione della posizione lavorativa: |       |
| Data: |       |
| Firma: |       |

# Organizzazione nel settore della sicurezza IT

| 1.1 | La vostra azienda dispone di un certificato valido e riconosciuto da un ente specifico del settore nel campo della sicurezza informatica (ad es. ISO27001 / CoBit / BSI ecc.)? | Sì ☐No ☐Non lo so☐ |
| --- | --- | --- |
|  | In caso di risposta affermativa, vi preghiamo di fornire una descrizione:  |       |
| 1.2 | Come è organizzata la sicurezza informatica nella vostra azienda? Descrivete le funzioni dei collaboratori nell’ambito della sicurezza informatica e specificate anche la persona responsabile di questo settore (CISO, IT Security Officer, CTO, ecc.): |       |
| 1.3 | Avete un sistema di gestione delle vulnerabilità? | Sì ☐No ☐Non lo so☐ |
| 1.4 | Attraverso quale canale e con quale velocità la vostra azienda informa la nostra organizzazione quando viene scoperta una vulnerabilità? |       |
| 1.5 | Attraverso quale canale e con quale rapidità la vostra azienda informa la nostra organizzazione in caso di incidente interno di sicurezza informatica? |       |

# Organizzazione nell’ambito della sicurezza dei dati

| 2.1 | La vostra azienda rispetta i requisiti e le specifiche della legge sulla protezione dei dati (LPD) per quanto concerne il trattamento dei dati? | Sì ☐No ☐Non lo so☐ |
| --- | --- | --- |
|  | In caso risposta affermativa, vi preghiamo di fornire una spiegazione:  |       |
| 2.2 | La vostra organizzazione dispone di un diagramma aggiornato che mostra come i dati sensibili entrano nei suoi sistemi e dove vengono archiviati? | Sì ☐No ☐Non lo so☐ |
|  | In caso di risposta negativa: la vostra azienda sarebbe disposta a creare un diagramma di questo tipo? | Sì ☐No ☐Non lo so☐ |

| 2.3 | La vostra azienda utilizza metodi di crittografia moderni, sottoposti a manutenzione e conformi agli standard industriali, per proteggere la trasmissione di dati sensibili tra sistemi nonché dati sensibili in quiescenza in supporti di dati e backup online? | Sì ☐No ☐Non lo so☐ |
| --- | --- | --- |
| 2.4 | La vostra azienda dispone di un concetto di distruzione dei dati (cancellazione definitiva dei dati)? | Sì ☐No ☐Non lo so☐ |
| 2.5 | Il fornitore ci fornisce prodotti IT od OT che operano nei nostri ambienti (critici)? | Sì ☐No ☐Non lo so☐ |
|  | Descrivere i prodotti IT/OT. |       |

# Sistemi informatici

| 3.1 | La vostra azienda utilizza sistemi dedicati per le prestazioni che ci vengono fornite?  | Sì ☐No ☐Non lo so☐ |
| --- | --- | --- |
|  | In caso di risposta negativa, se i sistemi sono forniti da fornitori terzi; di quale fornitore si tratta? |       |
| 3.2 | I sistemi sono dotati di una soluzione EDR/XDR aggiornata e gli incidenti rilevati da queste «soluzioni antivirus avanzate» sono gestiti attivamente presso la vostra azienda o controllati da un SOC esterno? | Sì ☐No ☐Non lo so☐ |
| 3.3 | È possibile ripristinare rapidamente il normale funzionamento di questi sistemi dopo un’interruzione del servizio o un incidente informatico? | Sì ☐No ☐Non lo so☐ |

# Accesso a sistemi informatici, altri dispositivi e workload

| 4.1 | Per accedere ai sistemi sopra descritti vengono utilizzati solo account utente personalizzati? | Sì ☐No ☐Non lo so☐ |
| --- | --- | --- |
| 4.2 | I vostri collaboratori utilizzano account utente diversi da quelli autorizzati ad accedere ai sistemi forniti dalla nostra organizzazione o a quelli contenenti dati della nostra organizzazione per svolgere il loro normale lavoro quotidiano?  | Sì ☐No ☐Non lo so☐ |
| 4.3 | Implementate l’approccio «least privilege» con i vostri collaboratori?  | Sì ☐No ☐Non lo so☐ |
| 4.4 | È garantito che gli account utente con privilegi elevati non abbiano permanentemente questo livello di autorizzazione? | Sì ☐No ☐Non lo so☐ |
| 4.5 | Se si utilizzano i cosiddetti «service-accounts» per fornire le prestazioni; è garantito che le credenziali siano conservate in modo sicuro e non siano accessibili a collaboratori non autorizzati? | Sì ☐No ☐Non lo so☐ |
| 4.6 | L’accesso ai sistemi che contengono/elaborano dati della nostra organizzazione è protetto da MFA in caso di accesso da zone esterne (tramite VPN o accesso intersito o simili)? | Sì ☐No ☐Non lo so☐ |
| 4.7 | Tutti gli accessi a questi sistemi sono registrati, protetti e possono essere visualizzati su richiesta dal personale addetto alla sicurezza informatica della nostra organizzazione? | Sì ☐No ☐Non lo so☐ |
| 4.8 | Esiste una politica scritta e dettagliata sulle password? | Sì ☐No ☐Non lo so☐ |

# Awareness

| 5.1 | I collaboratori sono stati sensibilizzati e formati in modo dimostrabile in materia di sicurezza informatica (almeno sulla minaccia del «phishing»)? | Sì ☐No ☐Non lo so☐ |
| --- | --- | --- |
| 5.2 | Un tale programma di formazione è accessibile al personale addetto alla sicurezza informatica della nostra organizzazione? | Sì ☐No ☐Non lo so☐ |