Credits: CSI Piemonte
segreteria@assintel.it

Dieci attività che un soggetto NIS 2 dovrebbe richiedere ai propri fornitori

Garantire la sicurezza e la conformità anche al di fuori del perimetro NIS 2

Introduzione

La Direttiva NIS 2 (Network and Information Security) stabilisce obblighi di sicurezza per le entità essenziali e importanti al fine di proteggere le infrastrutture critiche. Anche se un fornitore non rientra nel perimetro NIS 2, è cruciale che le entità soggette alla direttiva adottino misure preventive e richiedano specifiche attività per garantire la sicurezza delle informazioni e la continuità operativa. Di seguito sono riportate le dieci attività chiave che un soggetto NIS 2 dovrebbe richiedere ai propri fornitori.

1. Valutazione del rischio

Richiedere al fornitore una valutazione periodica dei rischi legati ai suoi processi, infrastrutture e servizi. Questa attività consente di identificare vulnerabilità e potenziali minacce che potrebbero impattare il cliente.

2. Implementazione di sistemi di sicurezza

Assicurarsi che il fornitore implementi misure di sicurezza adeguate, tra cui firewall, controlli di accesso, strumenti antivirus, VPN e sistemi di monitoraggio, per prevenire intrusioni e violazioni.

3. Gestione delle vulnerabilità

Richiedere un processo formale di gestione delle vulnerabilità che includa scansioni regolari, patching tempestivo e mitigazione dei rischi identificati.

4. Formazione del personale

Chiedere che il personale del fornitore riceva formazione periodica sulla sicurezza informatica, con particolare attenzione alle pratiche di protezione dei dati e alla gestione di incidenti.

5. Pianificazione della continuità operativa

Assicurarsi che il fornitore abbia un piano ben definito per garantire la continuità operativa in caso di incidenti, come cyberattacchi o disastri naturali. Questo include test regolari del piano e l'aggiornamento dello stesso.

6. Monitoraggio e reporting

Richiedere che il fornitore monitori costantemente i suoi sistemi e produca report dettagliati sulle attività, inclusi tentativi di accesso non autorizzato e altre anomalie.

Credits: CSI Piemonte
segreteria@assintel.it

7. Conformità normativa

Chiedere al fornitore di rispettare normative e standard di sicurezza applicabili, anche se non è soggetto diretto alla NIS 2. Ad esempio, potrebbe essere richiesto il rispetto di ISO 27001 o altre certificazioni rilevanti.

8. Gestione degli accessi

Assicurarsi che il fornitore gestisca gli accessi in modo sicuro, utilizzando sistemi di autenticazione multifattoriale e limitando i diritti di accesso ai soli utenti autorizzati.

9. Protocolli di risposta agli incidenti

Richiedere al fornitore di avere un protocollo ben definito per la gestione degli incidenti di sicurezza, che includa la comunicazione tempestiva con il cliente (entro le 24 dall'evidenza) e la risoluzione rapida del problema.

10. Audit periodici

Chiedere al fornitore di sottoporsi ad audit regolari per verificare l'efficacia delle misure di sicurezza implementate e identificare eventuali aree di miglioramento.

Conclusione

Anche se un fornitore non rientra direttamente nei requisiti della Direttiva NIS 2, la sicurezza delle informazioni e la protezione dalle minacce cyber sono responsabilità condivise. Richiedere queste dieci attività ai fornitori garantisce una maggiore resilienza e riduce i rischi per le entità soggette alla direttiva.