PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 26 - numero 5706 di Venerdì 04 ottobre 2024

Sicurezza informatica: anche i fornitori devono essere protetti

La sicurezza informatica è come una catena: ogni anello deve essere forte. Un programma interno valido non basta se i fornitori non sono altrettanto protetti. Ecco alcuni consigli utili dagli Stati Uniti per migliorare la sicurezza globale.

La National cybersecurity Center, negli Stati Uniti, ha messo a disposizione un prezioso documento, che offre a tutti i titolari di aziende uno strumento di verifica del livello di sicurezza della catena dei rifornimenti. Purtroppo, in fase di trattativa con un fornitore, non sempre si approfondisce il delicato tema, afferente alla sicurezza della catena di rifornimento, soprattutto a fronte di possibili attacchi informatici; il mancato tempestivo arrivo di un prodotto può bloccare una catena di produzione e quindi può avere riflessi assai gravi sulla produttività complessiva di un'azienda.

Ecco la ragione per la quale è opportuno che i responsabili della sicurezza informatica di un'azienda estendano la loro azione anche alla analisi della sicurezza informatica dei fornitori. L'agenzia federale americana ha messo a disposizione un piano di controllo in cinque punti.

1-Prima di cominciare

È bene effettuare un'analisi interna per verificare quali sono i fornitori critici per garantire la continuità produttiva o la fornitura dei servizi dell'azienda, individuando le strutture interne aziendali, che devono interfacciarsi con le strutture esterne, per garantire il costante mantenimento dei livelli di sicurezza informatica desiderati.

2-Sviluppare un approccio che permetta di valutare il livello di sicurezza informatica della catena dei rifornimenti

Occorre individuare quali sono gli aspetti critici della catena dei rifornimenti, che occorre mettere sotto attento controllo. Occorre poi mettere a punto una serie di profili di sicurezza per ogni fornitore, adottare metodi di verifica e controllo periodico del rispetto delle pattuizioni contrattuali, individuare i requisiti di sicurezza informatica, differenziati per criticità di fornitura, e via dicendo.

3-Applicate questo approccio ai nuovi contratti di fornitura

Occorre educare il futuro fornitore ad apprezzare il contributo che viene dato alla sua sicurezza, che indirettamente, costituisce anche contributo alla sicurezza dell'azienda committente. Occorre stabilire le condizioni contrattuali specifiche, e soprattutto i riferimenti alle tecniche di audit, sia di tipo periodico, sia di tipo non programmato, in modo da garantire che il fornitore rispetti questi temi critici.

4-Integrate questo approccio nei contratti di fornitura già in vigore

Probabilmente i contratti di fornitura già in vigore non danno un peso soddisfacente gli aspetti di sicurezza informatica; ecco perché occorre analizzare ogni singolo contratto già in vigore ed individuare, congiuntamente al fornitore stesso, quali siano le clausole contrattuali da aggiornare.

5-Avvio di un programma di continuo miglioramento

Una caratteristica dei sistemi informatici e della cybersicurezza è quella legata alla continua evoluzione della situazione, sia perché i malviventi si evolvono, sia perchè possono apparire nuovi punti di debolezza, precedentemente non individuati. Ecco perché occorre tenere sotto stretto controllo le informazioni che vengono dal campo, afferenti a nuove tecniche di attacco informatico e potenziali debolezze dei sistemi esistenti, in modo da adottare al più presto appropriate misure di controllo.

A questo punto, buon lavoro a tutti!

Adalberto Biasiotti

---

www.puntosicuro.it