2cents on Security

Pillole di Cyber Sicurezza

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

#7 I PROSSIMI PASSI SULLA NIS 2 PARTE 2

GESTIONE DEL RISCHIO:

Le organizzazioni devono adottare misure adeguate per gestire i rischi informatici, che includono, tra le altre, politiche di sicurezza, procedure per la gestione degli incidenti e procedure per il controllo degli accessi. In aggiunta, ruolo cruciale viene attribuito alle verifiche di sicurezza della supply chain da parte dei soggetti direttamente impattati.

NOTIFICA DEGLI INCIDENTI:

Gli incidenti significativi devono essere notificati al CSIRT Italia come segue:

1. pre-notifica, entro 24 ore;
2. successivamente, notifica entro 72 ore, che indichi una valutazione iniziale dell'incidente;
3. una eventuale relazione intermedia, su richiesta del CSIRT Italia;
4. infine, una relazione finale, entro un mese dalla trasmissione della notifica.

È prevista anche la possibilità di notifiche volontarie.

IL DECRETO PREVEDE SANZIONI SEVERE PER LE VIOLAZIONI:

10 milioni di euro per i soggetti essenziali o, se superiore, il 2% del fatturato annuo totale;

10 milioni di euro per i soggetti importanti o, se superiore, l'1.4% del fatturato annuo totale.

È previsto che le sanzioni vengano ridotte di un terzo nei casi in cui tali soggetti siano definiti come importanti e che la mancata notifica di incidente venga punita con sanzioni amministrative solo nel caso di reiterazione nell'arco di cinque anni.