Una vera cybersecurity prevede standard validi per tutti gli Stati


18

LaVerità

WELFARE AZIENDALE

Tempo per la famiglia nel lavoro del futuro

Terna chiude con le sigle sindacali un maxiprogetto integrativo. I dipendenti dell'azienda elettrica riceveranno un premio produttività, metà del quale potrà essere trasformata in servizi come asili e assistenza. Ma anche in giornate da dedicare ai figli

LE NOVITÀ

Premio di risultato 2017-2018

Da un minimo di 100 euro a un massimo di 3.000 di incremento spalmato nel triennio

Il premio di risultato si andrà ad aggiungere alla quota prevista dal contratto nazionale di lavoro

2017 210 euro
2018 280 euro

A questi benefici si aggiungono altri 40 euro destinati al fondo di previdenza integrativa Fopen

Welfare di produttività

Conversione volontaria, fino al 50% del premio, in prestazioni di welfare

Nel caso in cui i lavoratori aderissero alla «conversione», l'azienda si impegna a incrementare gli importi di un ulteriore 12%

Gli altri benefici

★ Permessi retribuiti per i dipendenti padri (5 giorni in più rispetto alla norma di legge)

★ Permesso di mezza giornata per l'inserimento scolastico

★ Realizzazione di un asilo nido aziendale a Roma ed eventualmente in altre sedi

Terna

Il nostro Paese è al settimo posto per numero di intrusioni

Una vera cybersecurity prevede standard validi per tutti gli Stati

Alberto Tripi (*)La Cybersecurity è la priorità assoluta: l' industria italiana va protetta con una strategia nazionale efficace che coinvolga tutti gli stakeholders. Solo una cooperazione a livello Ue globale può portare sicurezza al sistema Paese. Diffusione e pervasività delle tecnologie digitali offrono una grande opportunità al mondo produttivo ma possono esporlo a notevoli rischi. L' industria, motore della nostra economia, nella fase 4.0 vede interagire le nuove tecnologie informatiche (Ict) con il mondo fisico della produzione e della manifattura. Il ricorso all' Ict favorisce lo sviluppo di nuovi modelli di business, aumenta la competitività, può velocizzare la produzione, incrementare audience e fatturato, far dialogare le imprese con istituzioni e cittadini, ma espone ai «cyber criminali» che cercano di sottrarre dati, commettere frodi e compromettere il funzionamento di strutture critiche. L' Italia, seppur ancora indietro per l' uso di tecnologie digitali, risulta in prima linea come oggetto di truffe e ricatti online. Secondo lo studio di Trend micro The cost of compromise, siamo il settimo Paese nel mondo e il secondo in Europa più colpito dai ransomware, le estorsioni informatiche che bloccano un dispositivo a fronte della richiesta di un riscatto.La cybercriminalità porta un notevole danno economico: l' impatto è cresciuto di cinque volte tra il 2013 e il 2017 ed è previsto in forte aumento entro il 2019. L' affermazione dirompente dell' Internet delle Cose e la straordinaria velocità di diffusione di ogni nuova tecnologia (si calcola impieghi circa 35 giorni per raggiungere una massa critica di 50 milioni di utenti), rendono tutto più esposto, soggetto ad attacco diretto o utilizzabile come ponte per sferrare assalti a strutture terze.Le tecnologie abilitanti vedono un uso sempre più duale, idoneo sia all' uso civile, industriale, sia a quello militare, in settori quali l' aerospazio, la

Riproduzione autorizzata Licenza Promopress ad uso esclusivo del destinatario Vietato qualsiasi altro uso

ANGQ Associazione Nazionale Garanzia della Qualità

difesa e la sicurezza. Questo sintetico quadro indica quanto la sicurezza delle reti, dei dati e delle informazioni diventi oggi una missione cruciale.Una priorità assoluta da affrontare rapidamente e di concerto non solo nella dimensione Paese bensì a livello europeo e, possibilmente, mondiale, per assicurare lo sviluppo competitivo e rafforzare la fiducia nelle tecnologie digitali nell' attuale processo di trasformazione verso Impresa 4.0.Come? Una risposta efficace a livello europeo richiede cooperazione tra tutti gli stakeholder, nonché la capacità dei singoli Stati membri di strutturare un' azione coordinata. L' efficacia delle soluzioni di cybersecurity è strettamente correlata all' interoperabilità e alla definizione di standard, certificazioni e regole comuni.Vanno subito definiti con chiarezza ruoli e responsabilità dei principali attori e un quadro condiviso su come organizzare la certificazione della sicurezza delle tecnologie digitali in Europa. In questa direzione va il percorso avviato in questi giorni dall' Ue per la revisione della strategia per la sicurezza informatica, che risale al 2013.La cooperazione tra pubblico e privato è fondamentale. Anche in termini di risorse. Il partenariato pubblico-privato sulla cybersecurity del 2016 ha portato a un aumento delle risorse destinate alla sicurezza delle reti di 1,8 miliardi di euro da qui al 2020. Negli Stati Uniti, tuttavia, sono stati investiti 17 miliardi di dollari solo per il 2017. Le attività di ricerca e sviluppo vanno favorite. Va stimolata la trasformazione digitale dell' industria. Va sostenuta la formazione di nuove professionalità in ambito digitale con competenze ad elevata qualifica.Confindustria ha un ruolo importante. Sta seguendo il processo di revisione della strategia, sia attraverso il gruppo di lavoro sulla cybersecurity, che ricomprende le Federazioni più coinvolte dalla sicurezza informatica, sia con l' attività della delegazione di Bruxelles. Sostiene l' iniziativa della commissione europea di rafforzare il mandato di Enisa, l' Agenzia dell' Unione europea per la sicurezza delle reti e dell' informazione. Supporta lo sviluppo di meccanismi di finanziamento e incentivo per la realizzazione di piattaforme aperte volte a rendere accessibili strumenti di difesa altrimenti irraggiungibili dalle piccole aziende.L' obiettivo è permettere a tutte le imprese, grandi e piccole, un salto digitale in sicurezza.(*) Presidente del gruppo di lavoro cybersecurity della Confindustria e di Almaviva.

Riproduzione autorizzata Licenza Promopress ad uso esclusivo del destinatario Vietato qualsiasi altro uso