CyberRisk Evaluation

Il servizio CyberRisk Evaluation, attraverso una puntuale attività di verifica ed analisi dei dati, ha l'obiettivo di fornire un riscontro credibile sull'effettivo grado di rischio di attacco cyber delle Organizzazioni, identificando i gap rispetto a *best practices* e normative di settore.

I principali destinatari del servizio CyberRisk Evaluation sono tutte le aziende che considerano la corretta gestione degli asset informatici una questione di estrema importanza e che sono interessati a proteggere i propri asset da eventuali attacchi esterni attraverso l'utilizzo di strumenti di monitoraggio e analisi preventive basate su competenze specifiche. In particolare:
Aziende del settore Banking e Insurance con l'obiettivo di proteggere le transazioni finanziarie e l'integrità dei dati dei propri clienti e migliorare la credibilità e fiducia dei consumatori perché consapevoli che se il rischio cyber è monitorato si possono evitare perdite economiche per le banche, per i correntisti e le aziende corporate.
Aziende del settore Transportation con l'obiettivo di monitorare le vulnerabilità dei sistemi automatizzati di automezzi, velivoli e treni, in quanto il rischio di un eventuale cyber-attack può minare la sicurezza dei trasportati.
Aziende del settore Sanitario con l'obiettivo di monitorare le vulnerabilità dei sistemi automatizzati, principalmente per quanto riguarda i software medicali, al fine di garantire alti livelli di sicurezza dei pazienti.
Multinazionali o grossi gruppi di aziende con l'obiettivo di monitorare in modo accentrato le vulnerabilità dei propri sistemi informatici distribuiti sul territorio o ramificati in diversi paesi, al fine di tutelare e salvaguardare il patrimonio aziendale nella sua globalità.

L'obiettivo del servizio di **CyberRisk Evaluation** è quello di identificare e analizzare i rischi di un'organizzazione nella sua complessità, in ambito cybersecurity, in un dato periodo temporale, attraverso strumenti di analisi e attività di valutazione on-site dei punti di forza e debolezza del sistema dei controlli messi in atto per prevenire i rischi.
Il servizio consiste in una attività di ispezione secondo la norma UNI CEI EN ISO/IEC 17020, tramite l'utilizzo di check list che comprendono sia gli aspetti generali che quelli specifici del settore di riferimento, e delle *best practices* di settore.
Il servizio è composto dai seguenti step:

Ufficio Commerciale Certificazione Sistemi
Kiwa Italia
certificazione.sistemi@kiwacermet.it
+39 0514593242

- Attività di assessment on-site dei controlli messi in atto da una azienda per prevenire i rischi cyber, attraverso l'utilizzo di check list di settore.
- Elaborazione dei risultati e produzione di un report per evidenziare il livello di rischio cyber del cliente ed i punti di forza sui controlli messi in atto per il campione ed il periodo di riferimento analizzato.

Ufficio Commerciale Certificazione Sistemi
Kiwa Italia
certificazione.sistemi@kiwacermet.it
+39 0514593242