REPORT PER L'AZIENDA

None Tua Azienda

REDATTO IN BASE AI DATI FORNITI IL:

13/07/2022

CODICE PER RECUPERARE IL QUESTIONARIO:

tuBOLgGrhu8OcSu

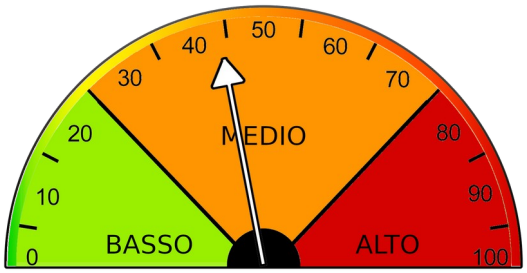
Se il questionario è stato compilato senza registrazione, la stringa qua sopra può essere utilizzata per recuperare le risposte ed eventualmente aggiornarle/modificarle

FINALITÀ DEL REPORT

Il presente report restituisce una valutazione in merito al livello di rischio cibernetico stimato per l'impresa ed elaborato sulla base delle riposte fornite al "PID-CyberChek" il test di autovalutazione online dei PID – Punti Impresa Digitale delle Camere di commercio realizzato con la collaborazione tecnica dell'Osservatorio di Cyber Security del CNR – Consiglio Nazionale delle Ricerche e del Competence Center START4.0.

Il test "PID-CyberCheck" potrà essere ripetuto in qualsiasi momento da parte dell'impresa generando di volta in volta un report aggiornato sulla base delle risposte fornite.

LIVELLO DI RISCHIO DI SICUREZZA INFORMATICA RILEVATO:



Livello del rischio: 44/100

Di seguito è riportata una breve descrizione dei quadranti di rischio inseriti all'interno della precedente figura che tengono conto delle risposte fornite al "PID-CyberChek":

RISCHIO BASSO	Un basso livello di rischio vuol dire che l'impresa ha intrapreso la strada corretta in tema di cybersecurity. Tale risultato non deve indurre l'impresa a ritenere di non aver bisogno di un esame approfondito che è fortemente consigliato.
RISCHIO MEDIO	Un medio livello di rischio indica che l'impresa ha ancora ampi margini di miglioramento in tema di cybersecurity. Un esame più approfondito dei sistemi aziendali è necessario per definire le politiche e gli interventi in materia di cyber security da mettere in atto.
RISCHIO ALTO	Un alto livello di rischio indica che l'impresa ha diverse criticità in tema di cyber security. Pertanto è fondamentale effettuare ulteriori approfondimenti, sottoponendo l'impresa a sistemi più approfonditi di analisi e attuare interventi per ridurre il rischio cibernetico.

La Tabella seguente riporta la stima delle perdite annuali previste per ogni minaccia e un valore sul rischio totale al quale è esposta l'impresa.

Tipo di Minaccia	Stima del Rischio (€)
Minaccia Interna	1615
Phishing	927
Glitch del Sistema	972
(D)Dos	16120
Furto di Hardware	411
Attacchi Web	8463
Attacchi alle Applicazioni Web	2895
Ransomware	8159
Negligenza degli Impiegati	221
Violazione/manomissione del sistema	8588
Inappropriatezza del sistema/ configurazione scarsa	130
Malware	4157
Danno Fisico	3835
Interruzione delle Comunicazioni	11
Rischio Complessivo	**56511.9 €**

LEGENDA

Minaccia Interna: questa minaccia è causata da un dipendente (o ex-dipendente) che ha accesso a parte del sistema e abusa di questi diritti.

Phishing: Il phishing è il tentativo fraudolento di ottenere informazioni sensibili come nomi utente, password e dettagli della carta di credito camuffandosi da entità fidata in una comunicazione elettronica.

Glitch del Sistema: un problema tecnologico (ad esempio, un problema di integrazione o errore imprevisto) che compromette la sicurezza informatica.

(D)Dos: mira a "bombardare" il servizio selezionato con un'enorme quantità di richieste che rendono il servizio non disponibile per gli utenti legittimi.

Furto di Hardware: furto fisico di apparecchiature, che possono contenere informazioni importanti o essere essenziali per la fornitura del servizio.

Attacchi Web: questa minaccia prende di mira gli utenti dei servizi, attirandoli e sfruttando le vulnerabilità dei loro computer. L'autore dell'attacco spesso sfrutta un servizio web per propagare alcune funzionalità dannose .

Attacchi alle Applicazioni Web: un utente malintenzionato sfrutta le vulnerabilità di un servizio o di un sito Web per interromperlo, iniettare funzionalità dannose o accedere a dati sensibili.

Ransomware: il ransomware è un malware che una volta penetrato nel sistema crittografa le informazioni e richiede il pagamento di un riscatto per la capacità di decrittografarlo.

Negligenza degli Impiegati: questa minaccia si riferisce a diverse azioni ingenue di un dipendente che portano a una violazione della sicurezza (ad esempio, l'esposizione di informazioni sensibili).

Violazione/manomissione del sistema: questa minaccia include gli attacchi che iniziano con un utente malintenzionato che ottiene l'accesso fisico agli elementi del sistema della vittima.

Inappropriatezza del sistema/configurazione scarsa: un utente malintenzionato può penetrare nel sistema sfruttandone la scarsa configurazione (ad esempio, utilizzando credenziali predefinite o ottenendo l'accesso a un archivio dati non protetto).

Malware: è un software progettato per causare interruzioni, divulgare informazioni riservate, ottenere accessi non autorizzati e altre azioni dannose.

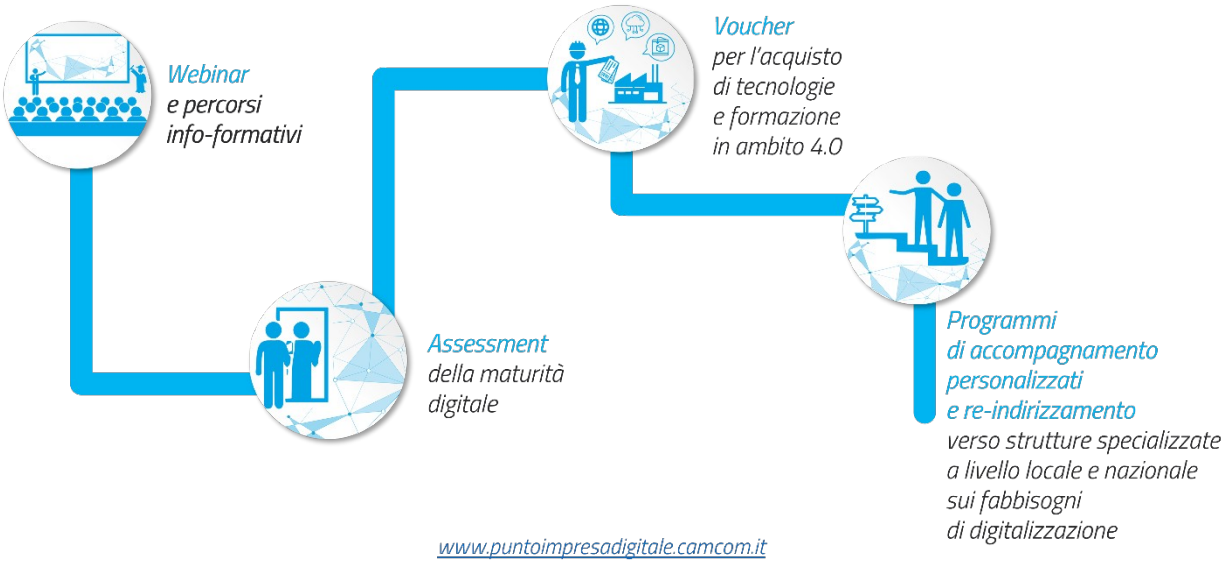
Danno Fisico: danno fisico dell'hardware che provoca perdità di integrità e disponibilità delle risorse digitali.

Interruzione delle Comunicazioni: questa minaccia mira a intercettare o manomettere la comunicazione tra le parti comunicanti. Un utente malintenzionato può trovare un modo per decifrare la comunicazione (senza crittografia o con crittografia debole) o sfruttare le vulnerabilità di protocolli non sicuri.

Vi ricordiamo che è possibile effettuare un assessment più approfondito che vi permetterà di capire più nel dettaglio la vostra esposizione digitale in termini di servizi esposti, di vulnerabilità e data leakage ("fuga di dati") denominato **Cyber Exposure Index**.

Tutte le informazioni le potete trovare al seguente link: www.puntoimpresadigitale.camcom.it.

CONTATTA IL PID – PUNTO IMPRESA DIGITALE DELLA TUA CAMERA DI COMMERCIO PER CONOSCERE ALTRE ATTIVITÀ SUL TEMA DELLA CYBERSECURITY E TUTTI I SERVIZI OFFERTI PER FAVORIRE LA TRANSIZIONE DIGITALE DELLA TUA IMPRESA



Disclaimer

Le informazioni contenute in questo report sono elaborate a partire dai dati forniti autonomamente dal soggetto che ha compilato il questionario per conto dell'impresa e non sono state oggetto di verifiche da parte di CNR, DINTEC Scrl, Infocamere, START4.0 o da altro Ente coinvolto nella sua realizzazione e promozione. Si informa pertanto che il risultato del presente report sul livello di rischio a cyber attacchi dell'impresa è fornito a puro titolo informativo senza alcuna garanzia esplicita o implicita di alcun tipo e non costituisce una certificazione e una analisi accurata dei sistemi di difesa dell'azienda.

Le strutture coinvolte nella progettazione e realizzazione del presente questionario si riservano il diritto di apportare cambiamenti, senza preavviso e in qualsiasi momento, al questionario ed ai risultati da esso generati.