REPORT PER L'AZIENDA

Nome della Tua Azienda

REDATTO IN BASE AI DATI FORNITI IL:

06/12/2022

CODICE PER RECUPERARE IL QUESTIONARIO:

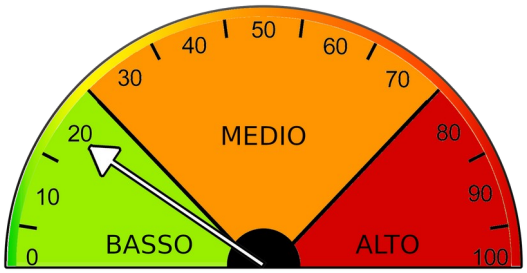
Se il questionario è stato compilato senza registrazione, la stringa qua sopra può essere utilizzata per recuperare le risposte ed eventualmente aggiornarle/modificarle

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: 19/100

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	13474
Phishing	182952
Glitch del Sistema	67684
(D)Dos	77665
Furto di Hardware	20714
Attacchi Web	49886
Attacchi alle Applicazioni Web	220328
Ransomware	1172648
Negligenza degli Impiegati	140840
Violazione/manomissione del sistema	2267
Inappropriatezza del sistema/ configurazione scarsa	49392
Malware	139085
Danno Fisico	920
Interruzione delle Comunicazioni	120
Rischio Complessivo	**2137981.08 €**

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.

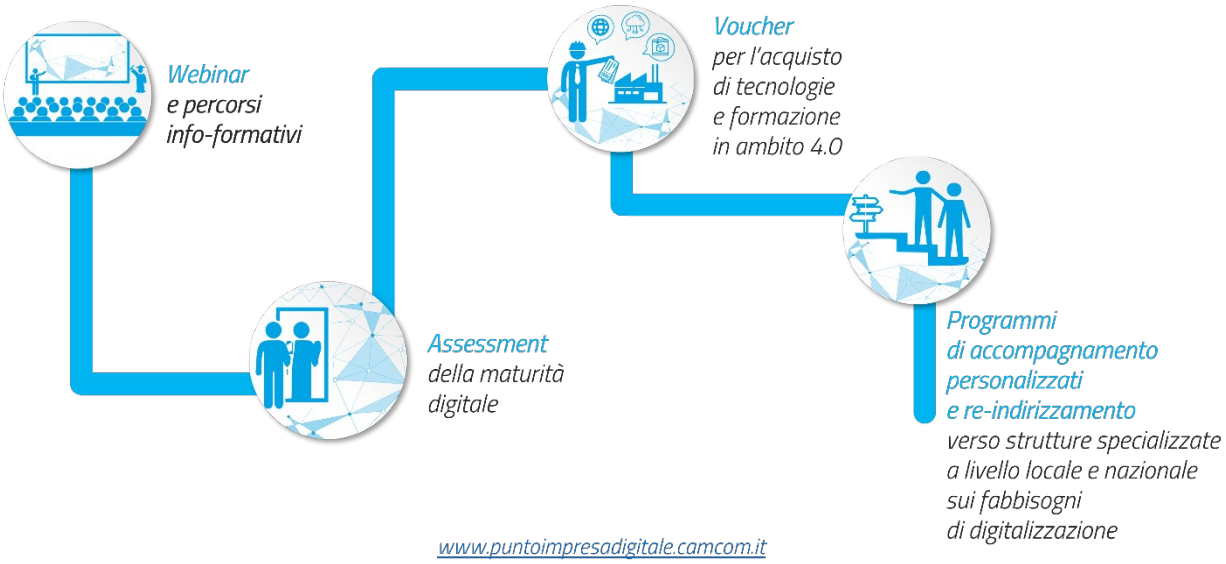
Interruzione delle Comunicazioni: questa minaccia mira a intercettare o manomettere la comunicazione tra le parti comunicanti. Un utente malintenzionato può trovare un modo per decifrare la comunicazione (senza crittografia o con crittografia debole) o sfruttare le vulnerabilità di protocolli non sicuri.

Vi ricordiamo che è possibile effettuare un ulteriore assessment che vi permetterà di capire 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 – **P**unto **I**mpresa **D**igitale 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.

Come funziona

Lo strumento PID-CyberCheck conduce una valutazione del rischio in conformità con le principali policies (ad es. ISO 27005, NIST 800-30, Octave Allegro, Magerit, RiskIT) di valutazione del rischio di sicurezza informatica.

Lo strumento raccoglie l'input dell'utente attraverso un questionario. Le risposte vengono utilizzate per approssimare i principali asset, vulnerabilità e perdite attese. Successivamente, lo strumento stima attraverso dei calcoli i rischi associati a minacce predefinite in base alle probabilità identificate e con le perdite previste. L'estrapolazione e il calcolo si basano sulle statistiche globali raccolte e aggregate.

Le statistiche utilizzate dallo strumento si basano su un'analisi di dati open source (NetDilligence [1], IBM Breach Cost [2], Wirpo [3], Simantec [4], Verizon [5], Enisa [6] e altri), nonché su dati commerciali più dettagliati. Le perdite stimate si basano anche su una serie di dataset sia disponibili online che privati. L'approccio computazionale è stato testato in progetti di ricerca [7,8].

I risultati rappresentano le perdite attese per un'organizzazione media di un settore specifico, stimate in base alle risposte fornite all'interno del questionario. Questi valori non indicano che l'organizzazione perderà definitivamente l'importo risultante in questo anno, ma rappresentano le possibili perdite a cui dovrà far fronte l'azienda in presenza di un cyber attacco.

I risultati devono essere considerati solo come indicativi e approssimativi, e hanno l'obbiettivo di supportare l'organizzazione a stimare l'ordine delle perdite, confrontare diverse minacce e identificare i rischi più importanti.

RIFERIMENTI

[1] NetDilligence, «Cyber Claim Study».

[2] IBM, «IBM Security Cost of a Data Breach Report».

[3] Wirpo, «State of Cybersecurity Report».

[4] Simantec, «Internet Security Threat Report».

[5] Verizon, «Data Breach Investigations Report».

[6] ENISA, «Report - Cybersecurity for SMES Challenges and Recommendations».

[7] A. Yautsiukhin, «Risk-based techniques and tools for Cloud Security Certification,» [Online]. Available: https://medina-project.eu/sites/default/files/D2.6_Risk-based%20techniques%20and%20tools%20for%20Cloud%20Security%20Certification%20%E2%80%93%20v1_v1.0_20220131.pdf.

[8] S. Dupont, A. Yautsiukhin, G. Ginis, G. Iadarola, S. Fagnano, F. Martinelli, C. Ponsard, A. Legay e P. Massonet, «Product Incremental Security Risk Assesment usinf DevSecOps Practices,» *SecAssure,* 2022.