CYBER SECURITY

La tua sicurezza informatica: un servizio di prevenzione e di pronto intervento

Più si è connessi alla rete, maggiore è il rischio di subire attacchi criminali e mettere a repentaglio la propria attività. **Punto Confindustria Srl** può rispondere alle esigenze di sicurezza delle organizzazioni, sia pubbliche che private, e valutare la sicurezza dei loro sistemi informatici prevenendo azioni che possono generare danni alla produzione o ai servizi che vengono offerti. I nostri servizi sono preventivi ed anche di ripristino in caso di emergenza.

FASE 1 - VALUTAZIONE DEL RISCHIO DI VULNERABILITÀ

EXTERNAL ANALYSIS. Connettersi e navigare in rete comporta elevati rischi per la sicurezza poiché espone il sistema informatico a svariate possibilità di attacchi dall'esterno.

- L'analisi individua i punti deboli specifici del sistema connesso a internet, verificando le vulnerabilità attraverso cui è possibile accedere alle informazioni riservate - personali e aziendali - e alle risorse dell'infrastruttura, sia a livello hardware che software.
- Dal singolo computer alle periferiche, fino agli apparati di rete come router, switch e firewall.
- Al termine di ogni analisi il cliente riceve un REPORT che evidenzia il livello di sicurezza dei servizi esposti sulla rete internet, i dettagli sulle vulnerabilità rilevate, le principali azioni correttive suggerite per incrementare il livello di sicurezza.

INTERNAL ANALYSIS. Le infrastrutture di risorse – software e hardware – connesse alla rete interna di un'azienda sono suscettibili di intrusioni al pari di quelle collegate a internet, sia che offrano la possibilità di accedere alla rete esterna, oppure no.

- L'analisi offre la possibilità di mappare l'architettura di rete e identificare con precisione i sistemi connessi tra loro e i software installati, perché i dati delle reti intranet sono una risorsa preziosa che richiede di essere custodita con la massima attenzione.
- Vengono forniti al cliente uno o più dispositivi hardware di piccole dimensioni che devono essere collegati alla rete interna aziendale. Ogni dispositivo attiva una connessione di rete sicura e crittografata verso il servizio di analisi di Punto Confindustria che si occupa della mappatura della rete, della identificazione dei software utilizzati e delle vulnerabilità.
- Il servizio può essere erogato in due modalità:
  - analisi singola
  - analisi ripetuta a intervalli di tempo concordati con il cliente.
- Al termine di ogni analisi il cliente riceve un REPORT che evidenzia il livello di sicurezza dell'infrastruttura informatica aziendale e riporta i dati relativi alle eventuali vulnerabilità identificate, le principali azioni correttive suggerite per incrementare il livello di sicurezza.

FASE 2 – INDIVIDUAZIONE DEI MIGLIORAMENTI DA APPORTARE

La valutazione conduce ad individuare le soluzioni tecnologiche ed i provvedimenti organizzativi da adottare per ridurre i rischi e migliorare il livello di sicurezza e di resilienza dell'infrastruttura informatica rispetto alle minacce ed alle vulnerabilità individuate nella fase precedente.

FASE 3 – ASSISTENZA NELL'ADOZIONE DEI PROVVEDIMENTI DI MIGLIORAMENTO

Un nostro tecnico può affiancare l'azienda nelle fasi di adozione dei provvedimenti individuati nella fase 2, come, ad esempio, stesura del manuale di sicurezza, scelta dei prodotti, installazione, configurazione e test.

FASE 4 – VALUTAZIONE DEL RISCHIO DI VULNERABILITÀ POST INTERVENTI

Si ripetono le external ed internal analysis per valutare l'efficacia degli interventi adottati e le risultanze sono esposte in un rapporto di sicurezza per la direzione aziendale.

PUNTO CONFINDUSTRIA

Punto Confindustria srl

info@puntoconfindustria.it
puntoconfindustria.it

Sede legale e operativa di Venezia
Via delle Industrie, 19
30175 Venezia Marghera (VE)
tel. 041.5499111

Sede operativa di Rovigo
Via A. Casalini, 1
45100 Rovigo (RO)
tel. 0425.2021

PRONTO INTERVENTO - ATTACCO INFORMATICO

Nel caso di incidenti informatici, è possibile analizzare le anomalie e risalire alle modalità in cui gli attacchi si sono verificati, analizzando le informazioni conservate nel sistema.
Il servizio consiste in:

- attività di prima risposta, analisi e mitigazione degli effetti di incidenti informatici
- conduzione di attività di digital forensics su dispositivi aziendali per approfondire le cause e le attribuzioni di un incidente informatico.

ATTIVITÀ DI FORMAZIONE

FORMAZIONE DI BASE. Corso per gli utilizzatori delle postazioni informatiche aziendali volto a sensibilizzare la necessità del rispetto delle tematiche di sicurezza informatica. Si svolge in modalità e-learning sviluppando i seguenti argomenti:

- **introduzione alla cybersecurity**: il concetto di cybersecurity, la sua importanza e quali sono i principali crimini informatici;
- **account e credenziali**: la gestione degli account e dei rischi che si corrono, con particolare riferimento alle best practice per la scelta delle password e per i sistemi di autenticazioni più forti, come, ad esempio, l'autenticazione a due fattori;
- **vulnerabilità hardware**: i rischi collegati ai dispositivi hardware, come ad esempio la compromissione di chiavette USB con malware e la loro diffusione e quali sono i comportamenti da adottare per proteggersi;
- **sicurezza Wi-Fi e VPN**: le problematiche relative all'uso delle reti Wi-Fi ad esempio per trasmettere dati sensibili mentre si è collegati a reti Wi-Fi pubbliche e quali sono i comportamenti da adottare;
- **social engineering**: che cos'è. quali sono gli attacchi che sfruttano questa tecnica, ad esempio il phishing, e come difendersi;
- **conclusioni**: sezione riepilogativa degli argomenti trattati.

FORMAZIONE FACOLTATIVA. Si tratta di 3 corsi da di 15 minuti ciascuno erogati con modalità e-learning sui seguenti temi:

- **attacchi informatici a tema Coronavirus**: si tratta di minacce che sfruttano la forte attenzione delle persone verso l'attuale pandemia;
- **truffa da supporto tecnico**: si tratta di minacce frequenti che sfruttano tecniche di "social engineering" per ingannare la vittima ed ottenere più informazioni sensibili possibile o l'accesso a sistemi informatici aziendali;
- **lavorare in sicurezza su ZOOM**: vengono presentati i meccanismi di sicurezza che dovrebbero essere adottati quando si utilizzano le applicazioni della videoconferenza.

SERVIZIO DI PHISHING

Si attuano campagne di white phishing periodiche per verificare le reazioni e il grado di consapevolezza raggiunto dalle persone a seguito delle attività formative svolte.

CONTRATTO TRIENNALE DI SUPPORTO CYBERSECURITY

Si tratta di un "abbonamento" che consente di avere attività periodiche di formazione, phishing e di pronto intervento per eventuali emergenze da cyber attack.

FINANZIAMENTI

Verifica con noi la finanziabilità del tuo progetto attraverso fondi nazionali, regionali e interprofessionali.

Lo sportello per le imprese: cyber@puntoconfindustria.it

Le aziende della provincia di Venezia e Rovigo interessate a fissare un appuntamento o a chiedere altre informazioni possono rivolgersi a:

NICOLETTA CASALICCHIO
Tel. 0425202234 – 3405719932 – n.casalicchio@puntoconfindustria.it – cyber@puntoconfindustria.it

PAOLA MUNARI
Tel. 0425202228 – 3357214867 – p.munari@puntoconfindustria.it – cyber@puntoconfindustria.it

PUNTO CONFINDUSTRIA

Punto Confindustria srl
info@puntoconfindustria.it
puntoconfindustria.it

Sede legale
e operativa di Venezia
Via delle Industrie, 19
30175 Venezia Marghera (VE)
tel. 041.5499111

Sede operativa
di Rovigo
Via A. Casalini, 1
45100 Rovigo (RO)
tel. 0425.2021