LE INFORMAZIONI VANNO TUTELATE

Nel settore della sicurezza occorre affidarsi a chi offre professionalità a 360 gradi In provincia di Brescia sono attive aziende che assicurano un servizio all'avanguardia

Dati aziendali sotto attacco Come proteggersi

Marco Lorenzi. Il presidente del Cda di Syneto

Syneto

■ Nel settore della cybersecurity servono professionalità e capacità di rispondere in modo efficace alle esigenze di ogni cliente. È questo ciò che offre Syneto, azienda bresciana esperta in infrastrutture IT, che ha fatto della competenza nell'ambito della sicurezza dei dati il suo punto di forza .

L'identikit. «Siamo fortemente legati al territorio - dice Marco Lorenzi, presidente del consiglio di amministrazione di Syneto - e ogni giorno mettiamo il nostro impegno nella sfida alla sicurezza informatica, orgogliosi di poter competere con i colossi americani e asiatici. Vogliamo tenere alta la bandiera di Brescia, dell'Italia e dell'Europa intera e democratizzare una tecnologia molto spesso ad appannaggio delle sole multinazionali. Il legame con Brescia è sempre vivo anche grazie alle partnership con i system integrator più importanti della provincia, come Tilak, Office Computers Solution, EcoElettronica, Beraid, Erecta AT, IT Core, Studio Archetti e Safeclick».

Le aziende che si affidano a Syneto hanno un'infrastruttura informatica tradizionale, in cui la funzione di data protection è gestita tramite backup. In questo caso però i sistemi sono vulnerabili e criptabili. «Facciamo migrare le imprese da un'infrastruttura tradizionale a una iperconvergente, con funzionalità avanzate di protezione dei dati nativamente integrate - prosegue Marco Lorenzi -. Il vantaggio reso possibile dal nostro software Syneto OS è fornire un numero quasi infinito di punti di ripristino che permettono a qualsiasi entità di dati di essere riportata istantaneamente in qualsiasi punto del passato». «Il vantaggio principale consiste nel combinare la semplicità di gestione con la capacità in caso di qualsiasi attacco informatico di ritornare in produzione in soli 15 minuti - conclude Marco Lorenzi -. Basta poco per recuperare i dati e fare ripartire la produzione aziendale». //

Soluzioni avanzate per la cybersecurity

Gi.One

■ Il 2022 è stato caratterizzato da numerosi attacchi informatici nei confronti delle aziende.

Tra i metodi più utilizzati c'è il phishing, truffa dove la vittima viene ingannata convincendola a fornire informazioni personali come dati finanziari o codici di accesso. Spiccano anche il social engineering, lo studio del comportamento di una persona al fine di estorcere informazioni, e il malware, che consiste nell'inserimento di un codice o un programma dannoso all'interno del dispositivo della vittima per sottrarre informazioni personali, password, denaro o per impedire agli utenti di accedere ai propri dispositivi. C'è stato inoltre un aumento di circa undici volte rispetto all'anno precedente di attacchi ransomware: un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto da pagare per rimuovere la limitazione (come i famosi cryptolocker).

I rimedi. La crescita esponenziale dei dati, la trasformazione digitale e l'industria 4.0 hanno aumentato la possibilità di subire un cyber attacco. È quindi necessario dotarsi di un sistema di sicurezza efficiente. Tra i principali strumenti di difesa ci sono firewall, soluzioni di intrusion preventions, monitoraggio It e business continuity.

Gi.One, in questi 40 anni di attività, ha stretto partnership con i migliori produttori di soluzioni sul mercato di cybersecurity, in modo tale da garantire sempre soluzioni complete e aggiornate. //

Ingest Srl - Piazzale Europa 30, 25068 Sarezzo (BS) - marketing@ingest.it - Tel: 0308930933

Una realtà consolidata e di qualità certificata

Invisiblefarm

■ L'Italia è il quarto Paese al mondo ad aver subito più attacchi informatici alle strutture sanitarie e ospedaliere negli ultimi mesi del 2021 e nei primi cinque del 2022.

Secondo i dati pubblicati dal rapporto Clusit, solo in questi mesi citati a cavallo tra i due anni si sono registrati più di 10 attacchi informatici rivolti a strutture sanitarie italiane. Invisiblefarm, consapevole dell'attuale situazione a livello nazionale e da sempre attenta in ambito cybersecurity ha adottato una policy improntata a un high level in questo ambito.

Per consolidare l'etica aziendale in materia di sicurezza, l'impresa ha svolto un percorso specifico finalizzato all'ottenimento della certificazione Iso 27001 come formalizzazione di un imprinting che già fa parte del dna di Invisiblefarm. L'azienda si sta certificando anche per Iso/Iec 27017, 27018 e 27701.

Punto di riferimento. In particolare, la Iso/Iec 27017 rappresenta il riferimento per i controlli di sicurezza generali per gli utilizzatori e i fornitori di servizi cloud, mentre la Iso/Iec 27018 fa riferimento ai controlli per i fornitori di servizi cloud pubblici che agiscono come responsabili del trattamento. La certificazione Iso 27701 riguarda il Sistema di Gestione delle Informazioni sulla Privacy.

Viene posta inoltre una forte attenzione per la qualità, da oltre quattro anni Invisibilefarm è infatti certificata Iso 9001. //