Attacchi informatici alle aziendeUmbre: testimonianza su Rai3 aBuongiorno Regione delpresidente della sezione ServiziInnovativi e Tecnologici diConfindustria Umbriaaa

Riportiamo il video dell’intervento a Buongiorno Regione del CEO Btree, Mariano Gattafoni, inqualità di presidente della sezione Servizi Innovativie Tecnologici di Confindustria Umbria, in cuitestimonia la reale minaccia ed i recenti attacchiinformatici subiti da alcune fra le più prestigioseaziende umbre.

Il messaggio di forte allerta si può riassumere nella considerazione che il rischio di essere presi di mira dagli hackers per le imprese non è ipotetico ma bensì è una questione di tempo.

Le conseguenze di un attacco informatico

Le conseguenze possono essere molto gravi come la perdita di dati, il blocco dei sistemi informatici con relativo fermo dell’attività aziendale, caduta di reputazione ed eventuale diffusione di dati personali coperti da privacy che può esporre alle sanzioni del Garante.

Perciò è necessario farsi trovare pronti, sia per respingere gli attacchi, sia nel caso riescano a bucare le difese per gestirli in maniera da minimizzare i danni.

Purtroppo, l’esperienza sul campo ed i dati ci confermano che, come 30 anni fa, la maggior parte delle imprese mette in atto un piano per la sicurezza informatica e di gestione dell’vento solo dopo aver ricevuto un attacco e quindi dopo aver subito ingenti danni.

Gli strumenti per la sicurezza informatica che ogni azienda dovrebbe adottare

Il presidente della sezione Servizi Innovativi e Tecnologici nel corso della breve intervista elenca, a beneficio anche dei non esperti, i più comuni e indispensabili strumenti di difesae l’importanza di prevedere procedure e responsabilità per la gestione e la comunicazione dell’evento malevolo, tra cui:

- uso di credenziali robuste (lunghe e complesse) e diverse per ogni applicazione;
- custodire in maniera oculata credenziali e password (meglio se si utilizzano strumenti di custodia sicura e criptata delle credenziali aziendali);
- aggiornare le password a cadenze prestabilite e comunque al sentore di una potenziale violazione;
- utilizzare sistemi di autenticazione a più fattori;
- formare e rendere consapevole il personale sui rischi e sull’utilizzo corretto del web,