Il caso MTS Srl

Federico Miatto


CYBER SECURITY


MA PUOI CAPIRE SE ATTACCANDO
UN'AZIENDA COME LA NOSTRA.
SIAMO A BOSCONERO.
MANCO GOOGLE MAPS SA TROVARCI

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).
United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: .....MITNICK, KEVIN DAVID
AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:
Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN

Kevin Mitnick, è stato l'hacker più ricercato del mondo. La fama del "Condor" è legata a una serie di crimini informatici e furti di dati commessi negli anni Novanta. Dopo aver scontato la pena divenne consulente per la sicurezza

La più grande minaccia per la sicurezza di un'azienda o un'organizzazione, amava dire Kevin Mitnick, non è un virus informatico o una falla nel software: "L'anello debole sono le persone"

COSE NON FATTE CHE HANNO PORTATO ALL'ATTACCO HACKER

La sicurezza informatica è una sfida costante e richiede un approccio proattivo.
Cose non fatte

Formazione del personale: Mancanza di adeguata formazione sulla sicurezza informatica.
Aggiornamenti regolari: Inadeguati e sporadici aggiornamenti di tutti i sistemi operativi, i software e le applicazioni. Spesso, le vulnerabilità sfruttate dagli hacker sono legate a software obsoleti o non aggiornati.
Backup regolari: Mancata esecuzione di regolari backup dei dati critici. Non corretta archiviazione in un luogo sicuro e offline. In caso di attacco ransomware, potrai recuperare i dati senza dover pagare un riscatto.
Protezione antivirus e antimalware: Non corretta installazione, aggiornamento e uso di programmi antivirus e antimalware su tutti i dispositivi.
Firewall: Inadeguata configurazione e manutenzione attiva di firewall sia a livello di rete che sui singoli dispositivi.
Politiche di accesso: Assenza di limitazioni di accesso ai dati sensibili solo al personale autorizzato
Monitoraggio dell'attività di rete: Totale assenza di strumenti di monitoraggio per rilevare attività sospette sulla rete.
Autenticazione a due fattori (2FA): Assenza di autenticazione a due fattori ovunque possibile
Pianificazione per la risposta agli incidenti: Assenza di un piano di risposta agli incidenti per affrontare tempestivamente e in modo efficace eventuali violazioni della sicurezza.
Collaborazione con esperti di sicurezza informatica:
Nessun rapporto di consulenza con esperti di sicurezza informatica per eseguire test di penetrazione e valutare la sicurezza del tuo sistema.

Ricorda che la sicurezza informatica è un processo continuo e dinamico.
È importante mantenere una mentalità vigile e adattabile per affrontare le minacce in evoluzione

COSE FATTE DOPO CHE LE MUCCHE SONO SCAPPATE DALLA STALLA

In generale, dopo essere stati vittime di un attacco informatico e aver pagato un riscatto per recuperare i dati, un'impresa dovrebbe adottare una serie di misure per prevenire futuri attacchi e migliorare la sicurezza informatica. Alcune azioni che potrebbero essere intraprese includono

1. **Analisi dell'attacco**: Effettuare un'analisi approfondita dell'attacco subito per capire come l'hacker è riuscito ad accedere ai dati e identificare eventuali vulnerabilità nei sistemi.
2. **Aggiornamento dei sistemi e dei software**: Assicurarsi che tutti i sistemi e i software siano aggiornati con le ultime patch di sicurezza. Le vulnerabilità note vengono spesso corrette attraverso aggiornamenti software.
3. **Miglioramento delle politiche di sicurezza**: Rivedere e potenziare le politiche di sicurezza aziendale, garantendo che siano robuste e aderiscano alle migliori pratiche del settore.
4. **Consapevolezza e formazione del personale**: Educare il personale sulla sicurezza informatica, sensibilizzandolo sugli attacchi più comuni come il phishing e insegnando loro come riconoscerli.
5. **Implementazione di un sistema di monitoraggio avanzato**: Installare sistemi di monitoraggio avanzato per rilevare comportamenti sospetti o intrusioni nel sistema in tempo reale.
6. **Backup regolari e procedure di ripristino**: Implementare procedure di backup regolari e testarle per assicurarsi che i dati possano essere ripristinati rapidamente in caso di un nuovo attacco.
7. **Crittografia dei dati sensibili**: Utilizzare la crittografia per proteggere i dati sensibili, rendendoli più difficili da accedere anche se un sistema viene compromesso.
8. **Accesso limitato e controlli di autorizzazione**: Limitare l'accesso ai dati solo al personale autorizzato e implementare controlli di autorizzazione per ridurre il rischio di accessi non autorizzati.
9. **Collaborazione con esperti di sicurezza informatica**: Coinvolgere esperti di sicurezza informatica per condurre audit periodici, identificare potenziali vulnerabilità e fornire consulenze sulla gestione della sicurezza.
10. **Pianificazione per la risposta agli incidenti**: Avere un piano dettagliato per la risposta agli incidenti in caso di futuri attacchi, con procedure chiare su come isolare l'incidente, comunicare con le parti interessate e ripristinare i servizi.

MA PENSA TE CI HANNO ATTACCA PURE A NOI, ANZI PROPRIO A NOI PERCHE' SIAMO IGNORANTI
(non c'è conoscenza sui cyberattacchi)
E PICCOLI.
Però almeno adesso ci siamo istruiti