ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4848 di Mercoledì 13 gennaio 2021

Anno bisesto, anno funesto: vale anche per gli attacchi informatici!

L'anno appena trascorso ha registrato non solo numerosi attacchi informatici, ma anche attacchi informatici di particolare gravità; ecco un riepilogo dei più significativi.

Abbiamo già dato più volte notizia degli attacchi informatici legati all'attuale pandemia. Gli attacchi illustrati di seguito non sono direttamente collegati a questo argomento, a dimostrazione di come il problema della sicurezza informatica stia diventando sempre più drammatico.

I lettori sono certamente già al corrente dell'attacco che ha coinvolto l'azienda di social media Twitter; in questo caso l'attacco è stato perpetrato mediante tecniche di social engineering. Gli attaccanti hanno potuto sottrarre i codici di accesso di parecchi dipendenti, introducendosi nel sistema informativo aziendale ed avendo accesso a numerosi profili di grandi personaggi, come Obama, Bezos, Musk e simili. In questo caso il riscatto è stato pagato in bitcoin, con un doppio guadagno per l'attaccante, perché il valore del bitcoin nel giro di poco tempo è salito in maniera esponenziale.

Un'altra azienda attaccata è una delle maggiori aziende che producono apparati di navigazione satellitare; anche in questo caso, l'attacco è stato di tipo ransomware di seconda generazione. Un attacco di prima generazione prevede solo il blocco dell'accesso ai dati, mentre l'attacco di seconda generazione prevede la cifratura dei dati aziendali, rendendo assai più difficile la ricostruzione dei dati, senza gli appropriati codici.

In questo caso attacco ha impedito all'azienda di mettere a disposizione dei clienti i numerosi aggiornamenti dei sistemi navigazione satellitare.

Un altro tipo di attacco, che ha colpito un cliente non particolarmente importante, ma che presenta un profilo affatto particolare, ha coinvolto il sistema informatico di una scuola degli Stati Uniti. In questo caso i malviventi hanno minacciato di rendere pubblici i dati degli studenti, se non veniva pagato il riscatto richiesto. In questo caso il numero dei soggetti coinvolti era relativamente ridotto, ma il profilo dell'attacco presenta aspetti decisamente atipici e particolarmente pericolosi, dal punto di vista di immagine e protezione dei dati personali.

Una gigantesca azienda di logistica è stata colpita due volte da attacchi con ransomware, a riprova che, anche se l'azienda aveva subito attivato adeguate misure di protezione, gli attacchi erano stati portati con due differenti modalità di ransomware, e l'azienda non era stata in grado di metterli rapidamente sotto controllo. Questo attacco ha messo in grave difficoltà non solo l'azienda, ma anche tutti i suoi clienti, perché è evidente che un'azienda di logistica opera in stretto contatto con i propri clienti e una anomalia negli archivi informatici ha immediate ripercussioni sul servizio reso. In particolare, gli esperti hanno rilevato una nuova variante di ransomware, chiamata Nelifilm.

A riprova che vi è una rincorsa continua fra le modalità di attacco le modalità di difese, anche una gigantesca catena alberghiera mondiale è stata due volte attaccata, in due anni. Questi attacchi hanno permesso di sottrarre informazioni afferenti a più di 5 milioni di clienti, che le utilizzavano per effettuare prenotazioni ed altre interazioni con la catena alberghiera. Tra queste informazioni c'erano purtroppo anche informazioni assai delicate, come ad esempio le carte di pagamento utilizzate, le informazioni sui passaporti, sui documenti di riconoscimento dei clienti e via dicendo.

Trattandosi di una catena alberghiera di grande prestigio, nessuno può dubitare che gli esperti informatici, dopo il primo attacco, si siano attivati al meglio ed il fatto che secondo attacco sia stato portato a buon fine dimostra come gli esperti informatici ancora rincorrono i malviventi informatici.

Un altro gigante, colpito il 12 maggio, è una compagnia di assicurazioni fra le più grandi del mondo, specializzata in polizze sanitario.

Anche in questo caso, sono stati catturati dati di più di 300.000 pazienti; l'attacco è stato perpetrato inviando un messaggio phishing, che sembrava essere originato da un cliente della compagnia di assicurazione.

Sono stati 20 i milioni richiesti per consentire di riprendere la piena funzionalità di una delle più grandi aziende di software del mondo, a riprova del fatto che non basta essere bravi informatici per poter dare credibili garanzie di resistenza ad attacchi informatici. Anche in questo caso, l'attaccante ha compiuto un salto di qualità, perché non solo ha impedito l'accesso ai dati aziendali, ma ha anche minacciato di rendere pubblici i dati sensibili afferenti ai dipendenti aziendali.

Ancora più raffinato è stato l'attacco condotto contro una grande azienda sanitaria finlandese, perché la richiesta di riscatto non è stata indirizzata all'azienda stessa, ma ai suoi clienti, i cui dati erano stati sottratti dai criminali informatici. In questo caso è intervenuto addirittura il ministro dell'interno della Finlandia, che ha convocato una riunione di emergenza del Consiglio dei Ministri, per offrire indicazioni ai clienti, vittime di questo tentativo di estorsione.

Particolarmente drammatico è stato l'attacco condotto contro una grande azienda, che vive proprio offrendo ai propri clienti strumenti di sicurezza informatica. In questo caso è stato appurato che l'attacco è stato portato da criminali informatici, riconducibili ad un particolare paese del mondo, alimentando così le polemiche che coinvolgono alcuni Stati, ormai ben individuati, che supportano queste tipologie di attacco.

Altrettanto grave è stato l'attacco contro un'altra azienda di sicurezza informatica, che ha compromesso anche i clienti dell'azienda stessa, in quanto il software di attacco è riuscito a introdursi nei sistemi informatici dei clienti stessi.

Se poi pensiamo che il 31 dicembre nientemeno che Microsoft ha rivelato che i malviventi si erano introdotti nella sua rete e avevano potuto esaminare il codice sorgente aziendale, ci rendiamo conto che la difesa contro attaccanti sempre più sofisticati diventa sempre più difficile.

Questa considerazione, ovviamente, non deve permettere di abbassare la guardia, seguendo un ragionamento del tipo: "tanto, se vogliono ci riescono!", ma deve spingere i responsabili della sicurezza informatica a sensibilizzare l'alta direzione sul fatto che occorre attivare e mantenere in essere un programma di costante aggiornamento delle misure di sicurezza informatica, nonché una buona polizza assicurativa.

Adalberto Biasiotti