01

PROTEGGERSI PRIMA DI UN ATTACCO

MANTENERE AGGIORNATI SOFTWARE E SISTEMI

"Gli aggiornamenti devono essere eseguiti costantemente e devono riguardare i PC Windows, ma anche i sistemi Linux e Mac, che possono costituire dei punti di accesso. È coinvolto l'intero parco informatico aziendale: da Microsoft Exchange ad Active Directory e tutti i server esposti, anche quelli di piccole dimensioni. ".

ESEGUIRE IL BACKUP DEI DATI… E PROTEGGERLO

"Questa precauzione da sola non è sufficiente, perché è la prima cosa che il ransomware cercherà di distruggere, prima ancora della crittografia. È necessario ricorrere a backup su nastro disconnessi dalla rete e stabilirne la frequenza. Occorre inoltre testare i ripristini per accertarsi che i backup siano utilizzabili. ".

PARTIZIONE DEL SISTEMA I NFORMATICO

"Si raccomanda di applicare regole rigorose sui flussi consentiti tra le diverse aree in base alla loro criticità. "

LIMITARE I DIRITTI DEGLI UTENTI E LE AUTORIZZAZIONI DELLE APPLICAZIONI

"Su questo punto, è la gestione nel tempo a essere decisiva: per garantire la sicurezza, è necessario pianificare controlli regolari. "

IMPLEMENTARE IL MONITORAGGIO DEI LOG

"La raccolta dei log rappresenta un obbligo. Nei casi in cui è richiesto un livello di sicurezza molto elevato, è possibile aggiungere un componente dirilevamento delle intrusioni tramite un SOC. "

SENSIBILIZZARE I COLLABORATORI

"Con l'ingegneria sociale, la principale porta d'accesso al sistema informatico di un'azienda è costituita dal suo personale. È quindi fondamentale affrontare i temi della cybersicurezza, anche se la sensibilizzazione ha i suoi limiti. "

ELABORARE UNA PROPRIA STRATEGIA DI COMUNICAZIONE PER LE CRISI INFORMATICHE

"Anche in questo caso, è utile aver definito in anticipo i messaggi e i contatti da utilizzare per comunicare in modo adeguato con i diversi tipi di destinatari. Tali comunicazioni servono ad avvertire, ad esempio, di interruzioni impreviste della produzione o di fughe di dati personali, come richiesto dal GDPR. "

IMPLEMENTARE UN PIANO DI RISPOSTA AGLI ATTACCHI INFORMATICI

"Questo piano è fondamentale, perché ci permette di reagire rapidamente, ad esempio contattando le organizzazioni CERT identificate in anticipo. Ovviamente include una componente tecnica, con l'implementazione di soluzioni di protezione come Stormshield Endpoint Security Evolution e Stormshield Network Security. "

VALUTARE LE OPPORTUNITÀ DI SOTTOSCRIVERE UN'ASSICURAZIONE CONTRO LE MINACCE INFORMATICHE

"Alcune polizze di cyber-assicurazione includono clausole sull'implementazione di soluzioni di sicurezza informatica; da questo punto di vista sono interessanti, perché impongono una certa protezione. Tuttavia, la cyber-assicurazione non dovrebbe essere vista come una misura di salvaguardia a sé stante, e ancor meno come una misura di protezione. In altre parole, l'assicurazione contro il ransomware non sarà mai una strategia di sicurezza informatica. "

Ransomware, quali sono le strategie da mettere in atto per smantellare questo meccanismo fraudolento?

Il ransomware è diventato il flagello dei reparti IT e delle aziende in generale. Ma è inevitabile? Abbiamo chiesto a Sébastien Viou, direttore della sicurezza informatica dei prodotti e cyberevangelista di Stormshield, quali misure adottare per far fronte alla situazione.

STORMSHIELD

03
RIPRENDERSI DA UN ATTACCO

RIPRISTINARE I SISTEMI DA SORGENTI SANE

INDAGARE IL PERCORSO DI ATTACCO

"Per valutare l'andamento dell'attacco e le debolezze del proprio sistema, bisogna analizzare ciò che è successo. Solo in questo modo potremo evitare che ciò accada di nuovo. "

ELABORARE UN PIANO CORRETTIVO

"A seconda dei casi, potrebbe rendersi necessario impostare un'autenticazione multifattore o migliorare le soluzioni di sicurezza presenti sulle postazioni di lavoro? "

INOLTRARE LA PRATICA ALLA COMPAGNIA DI ASSICURAZIONE

STABILIRE UN PIANO DI PRODUZIONE PER RECUPERARE IL RITARDO ACCUMULATO

INTRAPRENDERE UN'AZIONE LEGALE, SE NON È GIÀ STATA AVVIATA

GESTIRE L'IMPATTO PSICOLOGICO SUI DIPENDENTI

"Cassa integrazione, sensi di colpa, team IT sovraccarichi di lavoro: il ransomware determina conseguenze anche per le risorse umane, da tenere in considerazione". "

DIFFONDERE IL PIANO DI COMUNICAZIONE AI CLIENTI INTERESSATI, AI PROPRI INVESTITORI, ECC.

ASSICURAZIONE

PRESENTARE UNA DENUNCI

COMUNICARE AL GIUSTO LIVELLO

AFFIDARE LA GESTIONE DELLA CRISI INFORMATICA AL COMITATO ESECUTIVO

02
LIMITARE I DANNI DURANTE UN ATTACCO

AVERE DEI BUONI RIFLESSI

"Bisogna essere in grado di accorgersi rapidamente che qualcosa non va e non esitare a scollegare tutto per mitigare il rischio e contenere il più possibile la diffusione". Anche a livello individuale dobbiamo imparare a reagire, a dire "ho cliccato nel punto sbagliato", perché ogni minuto è importante. "