Luglio 2025

REGIONE MOLISE

Sistemi Informativi - Cyber Security Brochure

Ransomware

Il Malware che attacca e tiene in ostaggio i tuoi dati

Regione Molise - Servizio Sistemi Informativi e Transizione al Digitale

Progetto PNRR: M1C1I1.5 “Cybersecurity” formazione tecnica

Cosa troverai in questa brochure

Sommario

Introduzione

Negli ultimi anni, il **ransomware** – dall'inglese *ransom* ("riscatto") e *software* ("programma informatico") – si è affermato come una delle minacce informatiche più **gravi** e **diffuse**.

Il Ransomware è un tipo di attacco che **blocca l'accesso ai dati** o ai sistemi digitali di un'organizzazione, rendendoli inaccessibili e illeggibili, richiedendo al contempo un **pagamento economico** per ripristinarli.

Questa tipologia di attacco ha subito una rapida evoluzione: da episodi isolati e casuali si è passati ad azioni ben organizzate e mirate, rivolte anche contro enti pubblici, scuole, ospedali e infrastrutture nazionali. Le Pubbliche Amministrazioni, in particolare, sono diventate **obiettivi frequenti di attacchi Ransomware** a causa della grande quantità di dati gestiti e della rilevanza dei servizi offerti alla collettività.

Lo sapevi?

Nei primi 4 mesi del 2025, gli attacchi ransomware sono cresciuti del **+64%** rispetto allo stesso periodo del 2024*.

All'interno di tale contesto, l'**aumento della digitalizzazione** e l'uso più esteso delle tecnologie informatiche hanno reso le Amministrazioni più esposte a questo tipo di attacco. A fronte di questo scenario, è fondamentale che venga rafforzata la propria **resilienza digitale**, adottando strategie efficaci per contrastare il crescente pericolo rappresentato dal ransomware.

Le fasi di un attacco Ransomware

1. Accesso Iniziale
L'attaccante entra all'interno della rete.

2. Privilegi
L'attaccante ottiene tutti i permessi per svolgere attività malevole nella rete.

3. Furto dei Dati
L'attaccante copia e trasferisce i dati della vittima altrove.

4. Cifratura
L'attaccante rende inutilizzabili una parte o tutti i dati della vittima

5. Riscatto
Richiede alla vittima un pagamento per rendere di nuovo accessibili i dati.

***Fonte:** ACN - Operational Summary April 2025

Quali sono i rischi?

L'evoluzione delle minacce informatiche ha reso il **Ransomware** uno degli attacchi più **pervasivi** e **dannosi** per compromettere i sistemi informativi delle vittime. Tali attacchi sfruttano le vulnerabilità esistenti sui sistemi della vittima, esponendola a **rischi rilevanti**, quali:

Compromissione dei dati

A seguito di un attacco ransomware, la compromissione di dati sensibili rappresenta un **rischio rilevante**, poiché tali dati vengono prima **sottratti** e poi **resi inaccessibili alle vittime**. Ciò comporta gravi violazioni della riservatezza e responsabilità giuridiche.

Interruzione dei servizi

L'interruzione dei servizi si verifica quando i sistemi informatici della vittima vengono resi **inaccessibili**, impedendo lo svolgimento di attività essenziali. Ne derivano blocchi operativi, ritardi e disservizi ai danni di cittadini e del personale dipendente.

Danno reputazionale

La divulgazione della notizia dell'avvenuto attacco Ransomware e la conseguente diffusione pubblica dei dati possono **compromettere** in modo significativo la **reputazione** della vittima. La perdita di fiducia da parte di cittadini, istituzioni e media può generare un **danno d'immagine** duraturo.

Costi economici e legali

Un attacco ransomware può comportare **rilevanti costi diretti e indiretti**, legati al ripristino dei sistemi, all'assistenza tecnica e legale, nonché a eventuali sanzioni regolatorie. Tali oneri possono incidere gravemente sul bilancio economico della vittima e **rallentare** l'**operatività.**

Perché vengono utilizzare le criptovalute come pagamento del riscatto?

La nascita di **criptovalute**, come Bitcoin nel 2008, ha introdotto un'infrastruttura finanziaria che garantisce agli attaccanti **maggiore segretezza** e costi transazionali significativamente bassi.

Le criptovalute vengono ampiamente sfruttate nell'ambito degli attacchi ransomware poiché rendono più difficile **tracciare i pagamenti dei riscatti**: i criminali, infatti, utilizzano strumenti che nascondono l'origine e la destinazione del denaro, rendendo i **trasferimenti** più **anonimi** e quindi più **difficili da rintracciare.**

Come difendersi?

L'**inaccessibilità dei dati** blocca l'operatività dei sistemi e del personale, impedendo l'erogazione di servizi essenziali. Ciò causa **interruzioni** prolungate, perdita di produttività e impatti gravi sui processi interni.

Assicurati che vengano effettuati **backup regolari** dei dati e che vengano mantenuti al sicuro, in modo da poterli recuperare in caso di attacco.

La **pubblicazione** dei **dati esfiltrati** espone informazioni sensibili al pubblico o a soggetti malevoli, compromettendone la riservatezza e causando gravi danni reputazionali, legali e finanziari. Questo impatto può rivelarsi particolarmente critico per gli Enti pubblici ma anche privati

Valuta la **natura dei dati** che tratti: se essi sono riservati, poni **attenzione alla condivisione** dei dati e ricorrere a **metodi di comunicazione sicuri.**

Vulnerabilità non risolte nei sistemi, a causa di mancati aggiornamenti, rappresentano punti d'ingresso privilegiati per gli attaccanti, che possono sfruttarle per **infiltrarsi facilmente** nei sistemi ed eludere i controlli.

Quando i tuoi dispositivi (es. pc, tablet, telefono) richiedono l'esecuzione di un aggiornamento, **non rimandarlo.**

La maggior parte degli attacchi Ransomware ha origine dal **click sul link** da parte di utenti su **e-mail apparentemente legittime.** L'apertura imprudente di tali contenuti può consentire l'installazione del Ransomware che può propagarsi rapidamente e compromettere l'intero sistema.

Se ricevi un'e-mail che ti sembra sospetta, **non aprire allegati** e **non cliccare sul link** ma segnala prontamente l'accaduto.

Security Trends

maggio 2023

Ransomware all'ASL 1 Abruzzo: pubblicati dati sensibili

Nel maggio 2023, l'**ASL 1 Abruzzo** è stata vittima di un **attacco ransomware** condotto dal gruppo criminale Monti. L'incidente ha causato la cifratura dei server e l'esfiltrazione di circa **522 GB di dati sensibili**, tra cui cartelle cliniche, analisi genetiche, valutazioni psicologiche di minori e informazioni su pazienti affetti da HIV. Nonostante l'archivio principale sia rimasto integro grazie ai backup, i dati sottratti sono stati **pubblicati online** dopo il mancato pagamento del riscatto richiesto.

L'attacco ha paralizzato i servizi sanitari e amministrativi dell'ASL, costringendo il personale ad **operare** manualmente con **carta e penna** per diverse settimane. Il Garante per la protezione dei dati personali ha ingiunto all'ASL di comunicare il *data breach* a tutti gli interessati entro 15 giorni.

L'**Agenzia per la Cybersicurezza Nazionale** (ACN) ha valutato l'incidente come uno dei più gravi attacchi informatici recenti nel settore sanitario italiano.

In risposta, la Regione Abruzzo ha avviato una **revisione** delle misure di **sicurezza informatica**, migrando i sistemi delle ASL sul Polo Strategico Nazionale e implementando soluzioni avanzate per la protezione delle infrastrutture sanitarie.

Fonte: Garante Privacy - Ransomware Abbruzzo

dicembre 2023

Attacco ransomware a Westpole: disservizi per 1.000 enti pubblici

Nel dicembre 2023, l'infrastruttura cloud del fornitore **IT Westpole**, che fornisce servizi anche a realtà come **PA Digitale**, è stata colpita da un attacco ransomware condotto dal gruppo LockBit 3.0, compromettendo circa 1.500 macchine virtuali e causando l'interruzione dei servizi digitali per oltre **1.000 enti pubblici italiani**, tra cui ministeri, comuni e altre istituzioni locali come la **Regione Molise**.

L'attacco ha messo in evidenza la fragilità strutturale delle infrastrutture digitali delle pubbliche amministrazioni quando affidano i propri servizi a **provider esterni**, spesso condividendo ambienti critici senza adeguate misure di segregazione.

L'interruzione ha avuto ripercussioni immediate sull'erogazione di servizi essenziali alla cittadinanza.

L'incidente ha inoltre rafforzato il dibattito sull'**importanza della cybersicurezza** e sulla necessità di rafforzare le misure di resilienza digitale nella pubblica amministrazione, anche attraverso la vigilanza sui fornitori, il controllo dei contratti e una più attenta gestione del rischio di terze parti.

Fonte: Comunicato Stampa PA Digitale - ransomware Westpole

Grazie!

Per segnalare possibili minacce o problemi di sicurezza, od eventuali temi che vorresti approfondire scrivi a:

sistemi.informativi@regione.molise.it

Il presente Cyber Security Journal e tutti gli altri contenuti informativi a tema sicurezza informatica, sono disponibili all'interno dell'intranet di Regione Molise al seguente link:

"PERSONALE"