MUR
Ministero dell'Università e della Ricerca

CYBER SAPERE

Ransomware

I rischi di una minaccia in crescita e come essere preparati

Sommario

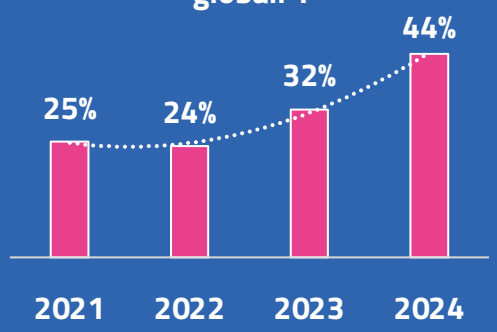
Cosa troverai in questa brochure

Introduzione

La **crescente digitalizzazione** ha reso la tecnologia **indispensabile** nella vita quotidiana e lavorativa di tutti noi, ma allo stesso tempo ha ampliato notevolmente la superficie di attacco sfruttabile dai criminali informatici per mettere a segno nuove e sempre più sofisticate truffe. Negli ultimi anni si è registrato un **aumento considerevole degli attacchi informatici**, caratterizzati da tecniche in continua evoluzione e da un impatto crescente, capace di colpire le grandi organizzazioni singoli utenti.

Tra le **forme di attacco** che hanno registrato un maggiore **incremento**, anche a danno delle **Pubbliche Amministrazioni**, spiccano i **ransomware**: malware progettati per **cifrare i dati e/o bloccare i sistemi informatici,** richiedendo un **riscatto** per il loro ripristino. Tali attacchi comportano **conseguenze** rilevanti sul **piano operativo**, **economico**, **reputazionale** e **legale**.

Percentuale degli attacchi Ransomware sul totale degli incidenti di sicurezza globali*:



Le fasi di un attacco Ransomware:

Accesso Iniziale:
L'attaccante entra all'interno dei sistemi sfruttando vulnerabilità tecnologiche o umane.

Privilegi:
L'attaccante ottiene tutti i permessi per svolgere attività malevole nei sistemi.

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

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

Riscatto:
L'attaccante potrebbe richiede alla vittima il pagamento di un riscatto per ottenere nuovamente accesso ai dati.

*Fonte: Data Breach Investigation Report – Verizon

Il fenomeno del Ransomware

Rischi

01 Interruzioni operative

La cifratura dei documenti può rendere inaccessibili dati e informazioni indispensabili per la prosecuzione delle tue attività, causando così il **rallentamento** o, nei casi più gravi, **l'interruzione dei processi e dei relativi applicativi**.

02 Compromissione Privacy

I criminali informatici, a seguito di un attacco ransomware, potrebbero **accedere** a **dati sensibili e strategici** e richiederti il pagamento di un riscatto per impedirne la diffusione. Tuttavia, le informazioni carpite, potrebbero essere divulgate sul Dark web, compromettendo così la tua riservatezza.

03 Danni Reputazionali

I possibili danni possono essere anche di tipo **reputazionale** in quanto la perdita o la diffusione non autorizzata di informazioni sensibili può minare la fiducia di dipendenti e/o possibili clienti, in virtù di una scarsa percezione di sicurezza nella gestione dei dati.

Contromisure

Pianifica regolarmente **backup** dei tuoi dati: in questo modo ridurrai il rischio di subire interruzioni operative in caso di attacchi Ransomware.

Non pagare mai il **riscatto** in quanto **non garantisce** il **recupero** dei dati sottratti né la loro diffusione sul Dark Web.

Non diffondere notizie al pubblico, **attieniti** alle **indicazione** di esperti e **autorità**.

Come difendersi?

Attenzione ai link e agli allegati sospetti

Evita di interagire con **e-mail sospette**, in particolare quelle provenienti da mittenti non attendibili che sollecitano azioni immediate o urgenti. Questi messaggi potrebbero rappresentare un tentativo di inganno.

Presta sempre **attenzione** a **link e allegati sospetti**: attraverso campagne di phishing, infatti, gli attaccanti possono diffondere malware di tipo ransomware, che una volta attivati possono accedere ai tuoi dati.

Verifica dispositivi rimovibili

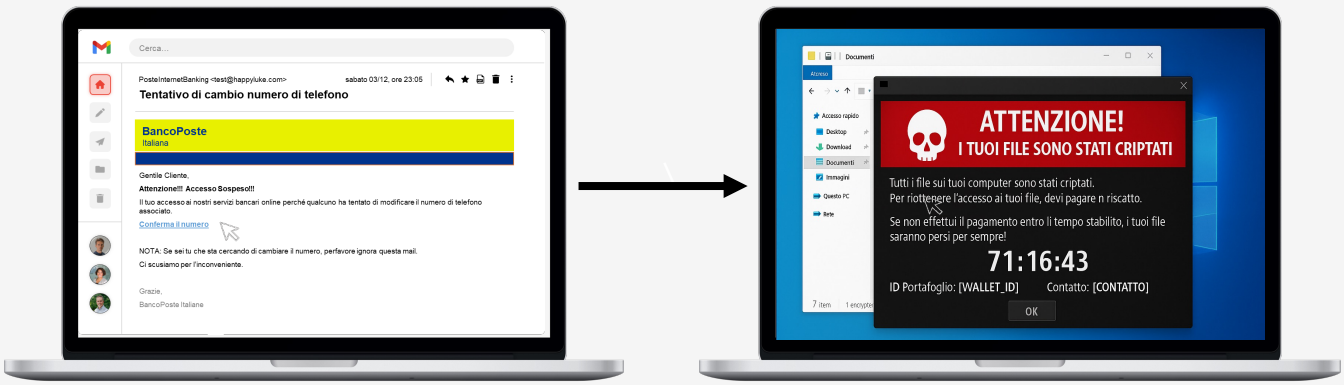
Evita di collegare **chiavette USB o periferiche di provenienza incerta** ai tuoi dispositivi personali o lavorativi.

In ogni caso, prima di utilizzare tali dispositivi rimovibili, **effettua sempre una scansione di sicurezza**: questa semplice precauzione può ridurre in modo significativo il rischio di diffusione di malware di tipo ransomware, salvaguardando così la sicurezza delle tue informazioni.

Back-up e protezione dei dati

Non **conservare i tuoi dati esclusivamente sul computer locale**, in quanto in caso di attacco ransomware rischieresti di perderli senza possibilità di recupero.
Per ridurre questo pericolo, **esegui backup regolari** e archiviali su **supporti esterni cifrati** o in **soluzioni cloud sicure**. In questo modo avrai sempre una copia di riserva disponibile e, in caso di cifratura di dati derivante da attacchi di tipo ransomware potrai ripristinare i tuoi file.

Esempio di Attacco Ransomware



Security Trend

Attacco all'Università di Modena e Reggio Emilia

Il **13 marzo 2025** il gruppo ransomware **FunkSec** ha rivendicato un attacco contro l'**Università di Modena e Reggio Emilia (UNIMORE)**, dichiarando di aver esfiltrato circa **1.000 file** dall'intranet universitaria.

Nei dati esfiltrati sarebbero presenti informazioni del progetto **U-Gov**, transazioni finanziarie, documenti interni e piani riservati, oltre a file **PDF, DOC, XLSX**, messaggi e caselle **Gmail** contenenti numeri di telefono.

Per dimostrare la veridicità dell'intrusione i criminali hanno pubblicato sul proprio **Data Leak Site** un primo pacchetto di prove, minacciando di diffondere il resto dell'archivio entro il **20 marzo 2025** in assenza del pagamento del riscatto.

Nelle ore successive, sui canali collegati al gruppo, sono comparsi estratti dei file sottratti e un **conto alla rovescia** che scandiva i giorni mancanti alla pubblicazione integrale, secondo la strategia ormai tipica della **doppia estorsione**.

L'episodio è stato segnalato anche dai **portali internazionali di monitoraggio ransomware**, che hanno inserito UNIMORE tra le vittime del mese di marzo.

marzo 2025

Ransomware colpisce l'Università degli Studi Roma Tre

Nella notte tra l'**8 e il 9 maggio 2025** è stato rilevato un attacco informatico, rivolto all'**Università degli Studi Roma Tre**, che ha provocato l'interruzione improvvisa di gran parte dei servizi digitali dell'Ateneo e ha reso **irraggiungibili siti istituzionali, piattaforme di didattica e servizi amministrativi** essenziali.

Nei giorni successivi l'Ateneo ha lavorato al ripristino delle funzionalità critiche: già dalla serata del **9 maggio alcuni servizi** sono tornati **accessibili**, consentendo una ripresa parziale di immatricolazioni, prenotazioni d'esame e consultazione dei dati accademici; tuttavia diverse procedure hanno **subito ritardi** e alcune attività sono state temporaneamente gestite con modalità alternative.

L'attacco ha inoltre compromesso il servizio centrale di **autenticazione**, determinando **sospensioni e rallentamenti** nelle operazioni quotidiane. I tecnici hanno operato in turni continui per **isolare le componenti compromesse**, **ripristinare** gli **accessi** e verificare l'**integrità** dei **sistemi**; contemporaneamente l'Ateneo ha attivato **comunicazioni ufficiali** alla comunità e **misure conservative** per garantire la continuità delle funzioni essenziali.

maggio 2025

MUR
Ministero dell'Università e della Ricerca

CYBER SAPERE

Restate sintonizzati:

nuovi approfondimenti sulla cybersecurity vi aspettano nelle prossime pubblicazioni.