White Paper

Ransomware: che cos’è e come difendersi

C’ERA UNA VOLTA IL VIRUS 2

L’AVVENTO DEL RANSOMWARE 3

COME DIFENDERSI DAL RANSOMWARE 5

CONCLUSIONI 7

C'ERA UNA VOLTA IL VIRUS

Di recente le discussioni su virus e minacce informatiche si sono intensificate a tal punto da diventare uno dei maggiori "trending topic" sulle più importanti testate giornalistiche nazionali e internazionali.

Anche se il fenomeno ha conosciuto grande diffusione solo negli ultimi anni, i virus non sono nati ieri.

All'inizio del 1999 c'erano virus come *Happy99* in grado di diffondersi via email e far comparire dei simpatici fuochi d'artificio che auguravano buon anno alle vittime. O ancora andrebbe citato il famoso *ILOVEYOU*, che prende il nome dall'oggetto delle email che venivano inviate alle mailing list delle ignare vittime.

Questi virus **erano innocui o poco pericolosi** e avevano come unico scopo quello di causare un effetto, quasi mai a scopo di lucro, sulle macchine delle vittime e diffondersi a macchia d'olio.

Ma allora **cos'è che li ha portati**, di recente, **a diventare così famosi e temuti**?

Ci sono almeno tre buoni motivi.

La diffusione di internet e lo sviluppo tecnologico

Se prima solo alcune attività aziendali erano affidate ai computer, con la diffusione di internet e l'ingresso definitivo nell'era digitale, tutto è cambiato: documenti, processi, dati personali, ogni cosa viaggia su internet o si trova su una macchina o un server, on premise o in cloud.

Di fatti, **man mano che le potenzialità di internet venivano scoperte**, man mano che la disponibilità di banda aumentava e i PC diventavano più performanti, **hanno cominciato a diffondersi virus** sempre più pericolosi.

Vale la pena citare tra i primi *SQL Slammer*, che nel 2003 ha seminato il panico bloccando oltre 75000 server e rallentando la navigazione su internet a livello globale.

La possibilità di monetizzare

La nascita e la diffusione delle criptovalute come il **Bitcoin** ha reso più facile lo scambio di denaro in forma anonima e sicura. Lo sviluppo del dark web come piattaforma di compravendita di dati ha poi contribuito a dare ancora più valore a dati sensibili violati e credenziali rubate.

Più valore hanno i dati per le aziende, più diventano un ghiotto bottino per i cyber criminali.

Criptovalute: valute virtuali decentralizzate caratterizzate spesso dalla garanzia dell'anonimato.

Dark web: parte del web non indicizzata dai motori di ricerca visitabile con navigazione anonima, quasi sempre utilizzata per attività illegali.

Virus polimorfi: virus in grado di alterare o offuscare una parte del proprio codice in modo da non essere riconosciuti dagli antivirus.

Firme antivirali: archivio contenente le "firme" dei virus, ovvero una sequenza di codice che li identifica e li rende riconoscibili da parte dell'antivirus.

I virus polimorfi e gli attacchi mirati

Come la storia ci insegna, quando emerge un'epidemia, studiosi e ricercatori si mettono all'opera per ottenere un vaccino efficace.

La stessa cosa è avvenuta nel corso degli anni con i virus: quando una minaccia veniva rilevata e iniziava a diffondersi, i **produttori di antivirus rilasciavano un nuovo aggiornamento contenente le firme per riconoscerlo e contrastarlo**. Banalizzando si può dire che le firme antivirali non sono altro che il vaccino per una determinata specie di virus.

Il problema è che **i virus sono cambiati**: i cyber criminali sono dotati di strumenti in grado di differenziarli e personalizzarli a tal punto che al giorno d'oggi **il 98% delle minacce è costituito da virus o malware unici** e specifici per ogni singolo PC.

Per rendersi conto della diffusione e del tasso di crescita di questi virus basti pensare che ogni 3 secondi compaiono 10 nuove minacce in rete.

In questo scenario **le firme degli antivirus non sono più uno strumento di difesa efficace**: ci vuole del tempo per aggiornare i software sui PC aziendali e, anche una volta fatto, ci saranno state diverse mutazioni e varianti dello stesso virus che lo avranno reso irrintracciabile.

L'AVVENTO DEL RANSOMWARE

Alla categoria delle minacce difficili da contrastare appartengono sicuramente i ransomware.

Che cos'è il ransomware

Un ransomware è un tipo di virus, diffusosi a partire dal 2013, che **ha come scopo quello di estorcere del denaro alle vittime**. Data la sua diffusione e la sua pericolosità può essere considerato la più importante piaga informatica del decennio.

Il virus si occupa di **cifrare tutti dati sui PC colpiti**, rendendoli illeggibili e inutilizzabili se non si è a conoscenza della chiave di decrittazione.

Una volta crittografati i dati, il virus mostra un messaggio sullo schermo del malcapitato, **chiedendogli di pagare un riscatto** (*ransom in inglese*) in criptovaluta, in genere Bitcoin, per riavere indietro i suoi dati.

Come si propaga l'infezione

Le modalità di infezione del ransomware hanno conosciuto uno sviluppo nel corso degli anni, ma quasi tutti questi virus hanno come vettore i messaggi di posta elettronica.

I primi ransomware puntavano spesso a sparare nel mucchio: i messaggi email che li veicolavano difficilmente erano personalizzati e presentavano spesso errori grammaticali evidenti.

Con il passare del tempo la tecnica si è affinata e i **messaggi sono diventati sempre più personalizzati**.

Oggi il metodo di infezione più comune prevede la ricezione di **un'email apparentemente innocua**, spesso riguardante una fattura o un ordine relativi a fornitori realmente esistenti, **che presenta un allegato o un link pericoloso**.

Questa email risulta creata a regola d'arte, con nomi e loghi di aziende famose o fornitori **spesso indistinguibili** da quelli presenti sulle **comunicazioni ufficiali**. Quasi sempre il messaggio non presenta più errori grammaticali degni di nota, quindi un occhio poco esperto potrebbe scaricare l'allegato o cliccare sul link presente nell'email e dare avvio all'infezione.

Cifratura e riscatto

Una volta avuto accesso ai PC, i ransomware cifrano tutti i dati presenti su quella macchina, rendendola inutilizzabile e chiedono all'utente di pagare una certa somma per lo sblocco dei dati.

Non c'è una richiesta di riscatto fissa per i ransomware, di solito questa **si basa sulla disponibilità economica dell'azienda** o dell'individuo colpiti. I cyber criminali fanno in modo di richiedere una somma alta ma non impossibile da pagare: si va quindi dalle poche decine di migliaia ai milioni di Euro in base a chi viene colpito.

Proprio perché non c'è una richiesta minima il ransomware può colpire aziende di ogni dimensione: dai piccoli studi professionali alle multinazionali, dagli studi dentistici alle organizzazioni statali.

A favorire la diffusione su larga scala del ransomware contribuisce anche **l'emergere del RaaS o Ransomware as a Service**. I cyber criminali mettono a disposizione dei virus già confezionati e pronti all'uso che possono essere reperiti facilmente sul dark web e acquistati da chiunque. Non è necessario essere particolarmente preparati dal punto di vista tecnico per utilizzarli e monetizzare. Una volta ottenuto il pagamento di un riscatto, una percentuale del guadagno viene di solito incassata da chi ha venduto il virus, che in questo modo non deve neanche sporcarsi le mani.

Dopo il pagamento del riscatto, chi ha realizzato o diffuso il virus ransomware può scegliere se fornire gli strumenti per dare avvio al processo di decrittazione dei file, che quindi tornano nuovamente leggibili. È tuttavia accaduto diverse volte che i cyber criminali abbiano incassato la somma richiesta e abbiano lasciato i sistemi IT bloccati.

I costi nascosti del ransomware

Quando si vanno ad analizzare i costi del ransomware per un'azienda, il prezzo del riscatto è solo la punta dell'iceberg.

Se il PC infetto è un device aziendale, quasi sempre i ransomware riescono a propagarsi all'interno della rete e a infettare PC, server e backup locali, paralizzando, di fatto, tutto l'IT aziendale.

Quindi, quando si calcolano i costi del ransomware, ciò che bisognerebbe prendere in considerazione è il **costo del fermo dei sistemi causato dal virus**. Spesso, in caso di ransomware, le aziende restano improduttive per giorni o settimane. Oltre a non poter produrre e fatturare, e quindi a bloccare le entrate per quel periodo, le aziende devono comunque sostenere tutti i costi infrastrutturali e quelli relativi al personale.

In più, in caso di indisponibilità del servizio al cliente, diventano quasi incalcolabili i danni d'immagine che può subire un'organizzazione. **In alcuni casi**, a seguito di un attacco ransomware, **alcune attività hanno dovuto addirittura chiudere i battenti**.

Il successo del ransomware

Da che mondo è mondo virus e malware sfruttano vulnerabilità di sistema per fare breccia nelle macchine e nelle infrastrutture IT. Quando viene scoperta una vulnerabilità, di solito, in breve tempo viene rilasciata una patch che la risolve e gli utenti possono tornare a dormire sonni tranquilli.

Il **ransomware**, invece, **basa gran parte del proprio successo sullo sfruttamento delle vulnerabilità legate al fattore umano**. Attraverso le email i cyber criminali riescono ad arrivare facilmente agli utenti. E sono gli utenti che intraprendono un'azione a scatenare l'infezione: un click sul link sbagliato, il download di un allegato pericoloso, e così via.

Quello che i ransomware cercano di fare è arrivare agli utenti con messaggi email contraffatti sempre più personalizzati, sempre più mirati e sempre meno distinguibili da quelli autentici.

Poiché non esistono patch per le persone, solo una formazione costante può aiutare a mitigare i rischi di infezione.

COME DIFENDERSI DAL RANSOMWARE

La soluzione per arginare il ransomware passa attraverso un mix sapientemente combinato di tecnologie, risorse umane e processi.

Le tecnologie di difesa

Probabilmente in azienda sono già presenti un firewall e un antivirus: si tratta di strumenti indispensabili, ma che da soli non sono sufficienti a combattere le minacce moderne.

È necessario adottare un approccio multistrato alla sicurezza, dotarsi quindi di una serie di strumenti che combinati possono aiutare le aziende a proteggersi.

1. *Assessment di rete:* Il primo elemento da cui partire è un **assessment di rete**: si tratta di un censimento che aiuta a individuare tutti i modi in cui le minacce possono entrare nel perimetro aziendale. Con queste informazioni è possibile stendere un piano di lavoro per andare a coprire tutte le possibili falle.

2. *Filtro antispam:* Sicuramente il firewall è un buon punto di partenza, ma poiché la quasi totalità degli attacchi ransomware in Italia arriva attraverso la posta elettronica, un **sistema antispam efficace** è assolutamente necessario. Questo sistema dovrebbe essere in grado anche di bloccare gli allegati potenzialmente pericolosi.

3. *Filtro per la navigazione:* Se gli utenti sono un po' indisciplinati e sono portati a cliccare facilmente su qualsiasi link, si può valutare l'installazione di un sistema di **controllo della navigazione** per evitare che il personale finisca su siti sospetti o compromessi.

4 *Gestione dei permessi:* Poiché i ransomware attaccano gli utenti, ossia sfruttano il loro comportamento, è assolutamente necessario che i **permessi degli utenti sui computer** e il loro livello di accesso alle informazioni sulle reti aziendali **siano controllati** e organizzati in modo tale che i danni di un'eventuale infezione possano essere mitigati.

5 *Azioni su sistemi operativi e software:* Anche **agendo sui sistemi operativi e sugli applicativi utilizzati in azienda** è possibile limitare la superficie di attacco: occorre installare sistematicamente le patch, disabilitare le opzioni che permettono l'esecuzione di script dannosi, disabilitare le macro nei documenti di Microsoft Office. Le macro sono delle azioni che è possibile automatizzare all'interno dei documenti Office e non sono quasi mai utili per le attività lavorative, per cui mantenerle disabilitate di default è un ottimo modo per tutelare gli utenti.

Le risorse umane

L'approccio tecnologico per minacce come il ransomware non basta, in quanto questo prolifera sfruttando l'anello debole della catena: il fattore umano.

Occorre quindi cercare di rinforzare questo anello in ogni modo possibile.

La prima cosa da fare per mettere in sicurezza l'azienda contro gli attacchi moderni è **coinvolgere tutto il personale, rendendolo consapevole** dello stato attuale delle minacce informatiche e che il suo comportamento può essere determinante nel prendere o evitare un'infezione.

A titolo di esempio alcune iniziative in grado di aiutare possono essere:

- **corsi di formazione** e aggiornamento periodici;
- **campagne di phishing simulate**: possono essere messe in atto simulando degli attacchi email tramite l'invio di messaggi contraffatti del tutto simili a quelli usati dai cyber criminali. In questo modo è possibile monitorare quanti e quali utenti cadono vittima di questi tranelli per focalizzarsi in modo più specifico sulla loro formazione.

I processi

Nell'epoca in cui viviamo tutte le misure esposte fino ad ora non bastano a stare sereni: **occorre prepararsi** al peggio, cioè **a subire un vero** e proprio **attacco ransomware** in grado di bloccare l'azienda.

Il modo migliore per prepararsi è mettere a punto un **piano di disaster recovery**, ovvero delle dettagliate procedure di ripristino in grado di descrivere tutte le azioni da intraprendere in caso di crisi per ripristinare i dati aziendali e riprendere l'attività lavorativa.

Un buon piano di disaster recovery dovrebbe puntare a **far ripartire i sistemi IT nel minor tempo possibile**, con il minor impatto possibile dal punto di vista operativo ed economico.

Occorre quindi capire:

- dove si trovano i dati critici;

- quali sono i sistemi critici che richiedono una ripartenza pressoché istantanea e quali invece possono essere riattivati in n secondo momento.

Avere un buon piano di ripartenza è l'unico vero modo per essere certi che, anche in caso di attacco, sarà possibile recuperare i dati aziendali senza pagare alcun riscatto perdendo.

CONCLUSIONI

Viviamo in un periodo storico caratterizzato da un forte sviluppo tecnologico, in cui spesso la sicurezza informatica non riesce a stare al passo con le evoluzioni hardware e software e non riesce a coprire tutte le loro falle di sicurezza.

In questo ambiente si muovono i cyber criminali, pronti a sfruttare a proprio vantaggio ogni vulnerabilità di sistemi informatici e persone.

E' sicuramente compito di vendor e fornitori IT fronteggiare le minacce informatiche, ma questi non possono riuscirci senza la **collaborazione di aziende e persone** nell'adozione delle giuste misure preventive, sia a livello tecnologico, sia a livello umano: solo così le aziende potranno lavorare con maggiore serenità, focalizzandosi unicamente su come portare avanti il proprio business.