ATTUALITÀ

Hackers: come difendersi. Protezione, mitigazione o accettazione del rischio?

di **Fondazione AIDR** · 11 novembre 2021, 13:33

di Vito Coviello, Socio AIDR e Responsabile Osservatorio Tecnologie Digitali nel settore dei Trasporti e della Logistica

Sappiamo tutti bene che i computer hanno cambiato la nostra vita nelle attività lavorative e in quelle private. Tutti i nostri dati sono ormai trasferiti su aree di memoria residenti nei vari dispositivi o sul cloud.

In molti casi per mantenere aggiornati i nostri documenti e renderli accessibili dai differenti dispositivi in nostro possesso, ci serviamo di applicazioni che consentono di archiviare i contenuti multimediali su server remoti condivisi poi dai vari dispositivi dell'utente: ad esempio il sistema iCloud Apple consente di archiviare e rendere disponibili in modalità sincrona i ns. dati tra iPhone, iPad, iPod touch, Mac e PC Windows.

Tutti i dati aziendali e privati sono quindi conservati nelle modalità di cui sopra, semplificandone di fatto la gestione e riducendo il carico fisico sui lavoratori. Ma non ci sono solo i benefici, sono purtroppo anche aumentati in modo esponenziale i rischi di furto di dati e di danneggiamento dei sistemi ad opera degli Hacker.

Esistono diversi tipi di hacker, classificabili anche per le differenti tipologie di attacchi e di tecniche che utilizzano.

Se ne elencano di seguito alcune tipologie:

- White Hat Hackers.
- Black Hat Hackers.
- Gray Hat Hackers.
- Script Kiddies.

- Green Hat Hackers.

1. **White Hat hacker**

La prima categoria è quella degli hacker professionisti che lavorano per i Governi e le organizzazioni con il compito di testare il livello di sicurezza informatica dei rispettivi sistemi: la loro attività di hacking ha lo scopo di identificare i punti deboli e di correggerli immediatamente per impedire i possibili attacchi esterni.

Questi hacker "etici" hanno il compito di prevenire gli attacchi, di proteggere e di assistere i governi, le organizzazioni e le aziende.

1. **Black Hat hacker**

Gli hacker black hat attaccano i sistemi per accedervi in modalità non autorizzata con la finalità di rubare o distruggere il sistema. Svolgono attività criminale e normalmente operano con lo scopo di trarre profitto dai dati rubati per venderli ad altri o per ottenere dei riscatti dalla stessa azienda al fine di sbloccarne l'utilizzo.

1. **Gray Hat Hackers**

Ci sono poi i Gray Hat hackers: sono hackers esperti ma agiscono per divertimento, sperimentando azioni per incrinare le difese delle reti e dei sistemi. Sono classificato come Gray Hat Hacker quando decidono di trarre un vantaggio personale.

1. **Script Kiddies**

Sono gli hackers dilettanti: cercano di hackerare i sistemi utilizzando script di altri hacker per attrarre le attenzioni.

I loro attacchi sono definiti con l'acronimo **DDoS** (Distribuited Denial of service) o **DoS** (Denial of service): indirizzano verso un determinato IP un traffico eccessivo fino a farlo collassare. Attaccano siti web con lo scopo di creare confusione e di bloccarne l'utilizzo.

1. **Green Hat Hackers**

Nella scala degli hackers sono quelli che stanno imparando a diventare veri hacker: cercano opportunità e sperimentano per crescere nel mondo dell'hacking.

La lista potrebbe allungarsi ancora, ma le tipologie di cui sopra sono abbastanza rappresentative del pericoloso fenomeno di hacking presente in un mondo che poggia sempre più ogni attività, ogni interesse politico, economico, sociale e industriale sulle reti e sul web, traendone indubbi

benefici ma esponendosi sempre più ai rischi di attacchi informatici.

Non desta stupore quindi che il Governo degli Stati Uniti abbia offerto una taglia di circa 10 mln di dollari per avere informazioni sul gruppo di Hacker noto come "dark side", che avrebbe condotto a maggio u.s. un attacco ransomware ad un vitale oleodotto lungo 5.500 miglia sulla costa orientale USA.

L'attacco informatico ha causato una interruzione del servizio della compagnia Colonial Pipeline causando una carenza di carburante per diversi giorni: sembrerebbe che per sbloccare la situazione sia poi stato pagato un riscatto di circa 4,4 mln in Bitcoin.

Gli attacchi di tipo ransomware stanno diventando sempre più frequenti perché bloccano di fatto le attività delle aziende attaccate e queste ultime nella maggior parte dei casi sono costrette a pagare un riscatto per poter riprendere le attività.

Le piccole / medie imprese spesso non si preoccupano molto della sicurezza informatica ed è per tale motivo che diventano il bersaglio preferito dagli hacker essendo i loro sistemi e le loro reti più facilmente attaccabili. Le loro aziende sono messe di fronte ad una terribile scelta: pagare per riavere la disponibilità dei dati o perderli per sempre.

Si calcola che solo in USA sia stato stimato un giro di affari di alcuni miliardi di dollari per il 2021 richiesti per il ripristino dei dati hackerati con il fenomeno dell'estorsione informatica.

La categoria dei "Black Hat Hacker" cresce sempre più rapidamente e questi gruppi stanno diventando vere e proprie sofisticate ed attrezzatissime organizzazioni in grado di mettere in ginocchio molte attività strategiche nel mondo.

Come avviene un attacco?

Sono molte le modalità con cui è possibile apportare un attacco Ransomware.

A volte il ransomware è distribuito attraverso le falle di sicurezza del sistema operativo di una determinata tipologia di dispositivi per poi infettare l'intero sistema aziendale senza che vi sia stata alcuna incauta azione dell'utente. Per esempio, le versioni precedenti di Microsoft Windows sono particolarmente vulnerabili quando non sono più supportate dalle patch di aggiornamento.

Altre volte un ransomware può essere attivato cliccando su di una mail di phishing o scaricando un allegato di posta elettronica: il virus una volta attivato può assumere il controllo di un computer o dell'intera rete.

Le tipologie di attacco sono sostanzialmente due:

- Criptografia dei dati dell'utente che non potrà più accedervi senza una chiave per decriptare i medesimi
- Il blocco dell'utente fuori dai propri dispositivi e non può accedervi, in questo caso si può rimediare con un intervento di un esperto di sicurezza.

Ci sono poi gli attacchi di tipo DDoS (Distributed Denial of Service): in questo caso l'hacker invia un potente flusso di traffico internet con lo scopo di rallentare il sistema attaccato fino anche a bloccarlo. Spesso si utilizza questo tipo di attacco per compromettere temporaneamente l'efficacia dei firewall e delle altre infrastrutture di sicurezza per avere il tempo di installare il ransomware.

Come difendersi?

Le organizzazioni e le aziende di grandi dimensioni hanno da tempo messo in atto ogni accorgimento per ridurre al minimo il rischio di attacchi informatici e per non farsi cogliere impreparati.

Sono soprattutto i **piccoli** e, spesso, anche i **medi imprenditori** i più vulnerabili se utilizzano rete e sistemi non adeguatamente protetti e, di conseguenza, più facilmente attaccabili.

In ogni caso pagare il riscatto sarebbe già un gravissimo danno, ma rinunciare allo sblocco dei dati potrebbe comportare consistenti perdite di business e, in casi estremi, anche la chiusura delle attività / dei servizi erogati.

Oltre alla mitigazione del rischio raggiungibile stipulando polizze assicurative, è necessaria la prevenzione e, quindi, pianificare ogni attività idonea per proteggere adeguatamente la rete e i sistemi aziendali e dare adeguata formazione agli utenti sul tema delle modalità di comportamento per la sicurezza e la protezione dagli attacchi informatici.

L'accettazione del rischio senza adeguati investimenti sul tema della sicurezza e senza la sua mitigazione per il tramite di polizze assicurative, può esporre una azienda a forti e pesanti conseguenti in caso di attacco.

Negli ultimi anni è cresciuta in modo esponenziale la percentuale di sottoscrizione di polizze assicurative a copertura degli attacchi informatici e la consapevolezza delle aziende di investire sulla sicurezza delle loro reti e dei loro sistemi.

Tra il 2020 e il 2021, in piena era COVID-19, è stato registrato il raddoppio delle polizze assicurative a protezione di attacchi ransomware in risposta al fortissimo aumento degli attacchi di questo tipo registrati nel periodo di osservazione.

È opportuno dare anche evidenza che le compagnie assicuratrici stanno ora rivalutando quanta copertura possono permettersi di offrire e quanto devono addebitare ai clienti.

Le compagnie prima di sottoscrivere una polizza chiedono prove dettagliate sulle misure di sicurezza informatiche adottate dall'azienda: ad esempio, il mancato utilizzo dell'autenticazione a più fattori che richiede all'utente di verificare sé stesso in più modi, potrebbe comportare un rifiuto alla sottoscrizione della polizza da parte della compagnia.

In chiusura nessuna azienda può fare a meno della rete e di internet per sviluppare e promuovere il proprio business e, pertanto, deve proteggersi dagli attacchi dei **black hat hackers,** nuova e pericolosissima categoria di ladri di questo secondo millennio.

Articolo pubblicato su Istituzioni24: https://www.istituzioni24.it/2021/11/11/hackers-come-difendersi-protezione-mitigazione-o-accettazione-del-rischio/

© 2026 Istituzioni24