****

**Documentazione caso di studio**

**Analisi e Gestione del Rischio**

**Organizzazione analizzata:**

**Amazon.com**



*Corso di laurea:* Sicurezza Informatica

*Docente:* Stefano Cervellera

*Alunna:* Francesca Annese

*Matricola:* 765761

**Indice:**

1. Introduzione
2. Contesto aziendale
3. Struttura organizzativa e organigramma
4. Malware distribuiti i servizi di Amazon
5. Valutazione del rischio
6. Asset
7. Minacce
8. Tabella Minacce-Asset-Probabilità
9. Impatto delle minacce sui parametri RID
10. Rischio intrinseco quantitativo
11. Controlli di sicurezza
12. Rappresentazione del rischio totale
13. Confronto tra RI(m,a) e R(m,a,c)
14. Attenuazione del rischio
15. Analisi qualitativa
16. Normalizzazione del rischio
17. Test statistici
18. Variabili casuali
19. Variabili casuali -Binomiali
20. Probabilità composta di Data Breach
21. Variabili casuali – Poisson
22. Conclusioni

**INTRODUZIONE**

Per questo caso di studio, l’azienda che ho deciso di analizzare è **Amazon.com**, un’azienda originaria degli USA che si occupa di e-commerce insieme ai servizi di cloud computing.

L’obiettivo è quello di determinare il livello di rischio all’interno di questa organizzazione.

In particolare quello che andrò a fare è una valutazione del rischio, ovvero una determinazione quantitativa e qualitativa del rischio associato a una situazione definita e ad una minaccia conosciuta detta pericolo; verrà effettuato un processo di normalizzazione e verranno applicati i controlli di sicurezza.

Il **rischio** è la potenzialità che un'azione o un'attività porti a una perdita o ad un evento indesiderabile.  
La nozione implica che una scelta influenzi il risultato. Le stesse perdite potenziali possono anche essere chiamate "rischi". Sebbene ogni comportamento umano sia rischioso alcuni hanno una percentuale di rischio maggiore.  
Per "rischio" possiamo indicare anche la distribuzione dei possibili scostamenti dai risultati attesi per effetto di eventi di incerta manifestazione, interni o esterni ad un sistema. In questa definizione, il rischio non ha solo un'accezione negativa (*downside risk*), ma anche una positiva (*upside risk*). Esso è definito dal prodotto della frequenza di accadimento e della gravità delle conseguenze (magnitudo).

Con il termine **valutazione del rischio** si fa riferimento alla determinazione quantitativa o qualitativa del [rischio](https://it.wikipedia.org/wiki/Rischio) associato ad una situazione ben definita e ad una minaccia conosciuta (detta "pericolo"). Una valutazione del rischio quantitativa richiede la determinazione di due componenti del rischio: la gravità di una potenziale perdita ("magnitudo") e la [probabilità](https://it.wikipedia.org/wiki/Probabilit%C3%A0) che tale perdita si realizzi.

Avviene sulla base di alcuni aspetti fondamentali (che verranno approfondito nel corso di questo caso di studio):

* Contesto
* Minacce
* Asset
* Vulnerabilità
* Controlli

Quando si parla di valutazione del rischio, si parla anche di **Risk Assessment**, che rispetto alla gestione del rischio indica la valutazione dello stesso; in particolare è volto a individuare e analizzare i rischi per capire quali siano le priorità di intervento e produrre poi azioni strategiche per contenerli o attenuarli.

È il punto fondamentale della strategia di gestione del rischio e al suo interno include altre fasi: identificazione del rischio; analisi del rischio; ponderazione del rischio, ovviamente fasi che devono essere precedute da una comprensione del contesto e dell’ambito in cui si valuta il rischio.

Gli attori del sistema sono tanti, in primo luogo il risk manager, con i riferimenti a livello tattico strategico e organizzativo interni, ma anche i fornitori esterni (se questi hanno sistemi di analisi e gestione di dati propri vanno anche valutati).

**CONTESTO AZIENDALE**

**Amazon.com** è un’azienda originaria degli USA che si occupa di e-commerce insieme ai servizi di cloud computing. La sua sede è **città di Seattle** nello stato americano di**Washington.** Amazon è stata una delle **prime aziende a offrire e vendere beni in Internet** su larga scala.

È riuscita a creare siti web completamente indipendenti per molti mercati in cui è presente in tutto il mondo come

* Canada, Australia
* Italia
* Spagna
* Paesi Bassi
* Brasile
* India
* Messico
* Germania
* Austria
* Francia
* Cina
* Giappone
* Stati Uniti
* Regno Unito e Irlanda

In questo modo, questa azienda è in grado di offrire i prodotti specifici di ciascuno di quei paesi.

**Amazon è la più grande azienda di vendita al dettaglio online del mondo**, dove puoi trovare praticamente tutto ciò di cui hai bisogno in quanto è molto sicuro che qualcuno lo stia vendendo.

**L'azienda Amazon è stata fondata nel 1994 da Jeff Bezos** dopo aver lasciato il suo precedente lavoro come vice presidente di DE Shaw & Co. nello stesso anno, quella società era una delle principali società di Wall Street.

Il 23 novembre 2010 viene lanciata la versione italiana di Amazon.

Inoltre, Amazon fornisce una serie di servizi:

* [*Amazon Prime*](http://www.amazon.it/provaprime?tag=gamspri02-21)*:* il servizio di spedizioni rapide e gratuite
* [*Amazon Prime Video*](https://www.primevideo.com/?tag=gamspri02-21)*:* il servizio di video in streaming
* [*Amazon Music Unlimited*](https://www.amazon.it/music/unlimited?tag=gamspri02-21): il servizio di musica in streaming
* [*Amazon Business*](https://www.amazon.it/?tag=gamspri02-21)*:* negozio online di Amazon.it creato esclusivamente per aziende ed imprenditori. Aziende di tutte le dimensioni possono creare un account aziendale gratuito e semplificare i loro processi di acquisto grazie al facile accesso ad oltre 250 milioni di prodotti per aziende, fatturazione automatica e strumenti per la gestione delle fatture, offerte per aziende, sconti sulla quantità e consegne rapide e affidabili.
* [*Kindle Unlimited*](https://www.amazon.it/kindle-dbs/hz/signup?tag=gamspri02-21)*:* servizio che ti permette di leggere quanto vuoi, scegliendo tra oltre un milione di titoli
* [*Amazon Lista Nozze*](https://www.amazon.it/wedding/?tag=gamspri02-21)*:* il servizio di lista nozze di Amazon.
* [*Amazon Prime Student*](http://www.amazon.it/joinstudent?tag=gamspri02-21)*:* l’abbonamento Prime per gli studenti che potranno così usufruire del servizio a metà prezzo.
* *Amazon Pantry*: i servizio consente di ordinare e ricevere la spesa a casa
* *Amazon Pay:* il servizio permette di pagare online con l’account amazon
* *Amazon Photos*: Uno spazio di archiviazione in cui salvare e tenere al sicuro le proprie foto e i video

In aggiunta a questi servizi ‘base’, in molti Paesi sono presenti dei servizi aggiuntivi e specifici, appunto, per quel Paese.

**STRUTTURA ORGANIZZATIVA E ORGANIGRAMMA**

La struttura organizzativa di Amazon consente un controllo completo sulle operazioni di e-commerce a livello globale determinando il modo in cui i dirigenti dirigono e influenzano le attività operative in varie aree aziendali, essa consente il controllo manageriale e le sue caratteristiche forniscono anche il supporto necessario per il lancio di nuovi prodotti Amazon nel mercato dell'e-commerce. In qualità di principale attività di vendita al dettaglio online nel mondo, Amazon deve mantenere una struttura organizzativa che supporti adeguatamente la sua espansione sul mercato. Una struttura aziendale in evoluzione potrebbe anche portare benefici ad Amazon, poiché l'azienda aggiunge più prodotti e gradualmente diversifica la propria attività.

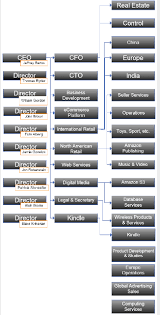
Amazon ha una struttura organizzativa funzionale. Questa struttura si concentra sulle funzioni aziendali come basi per determinare le interazioni tra i componenti dell'organizzazione. Caratteristiche più significative:

- Gruppi basati su funzioni globali

- Gerarchia globale

- Divisioni geografiche

I gruppi basati sulle funzioni sono la caratteristica più forte della struttura organizzativa di Amazon. Ogni funzione aziendale principale ha un gruppo dedicato insieme a un dirigente. L'obiettivo strategico è consentire ad Amazon di facilitare la gestione delle operazioni di e-commerce in tutta l'organizzazione. I principali gruppi basati sulle funzioni nella struttura organizzativa di Amazon sono:

- Ufficio del CEO

- Sviluppo del business

- Amazon Web Services (AWS)

- Finanza

- Affari internazionali dei consumatori

- Contabilità

- Affari dei consumatori

- Legale e segreteria

La gerarchia di Amazon è espressa in termini di un sistema globale di linee verticali di comando e autorità che influenzano la società di vendita al dettaglio online. Ad esempio, le direttive degli alti dirigenti sono applicate in tutta l'organizzazione, interessando tutti gli uffici competenti della società in tutto il mondo. L'obiettivo strategico di questa caratteristica della struttura aziendale è di facilitare il controllo manageriale dell'intera organizzazione di Amazon.

Amazon attua le divisioni geografiche che prevedono gruppi basati su regioni geografiche e obiettivi aziendali correlati. Le divisioni geografiche vengono utilizzate per semplificare la gestione dell'attività di e-commerce in base alle condizioni economiche di determinate regioni, per consentire all'azienda di affrontare problemi rilevanti per ciascuna regione geografica.

**MALWRAE DISTRIBUITI TRAMITE I SERVIZI DI AMAZON**

Secondo una ricerca condotta da Cisco Talos tra gennaio 2021 e gennaio 2022, sono state rilevate campagne malevoli che usano malware come Nanocore, Netwire e AsyncRAT per attacchi mirati distribuiti tramite i servizi cloud di AWS e Azure.

Nel tempo però ci sono stati vari episodi allarmanti che hanno colpiti vari servizi Amazon.

Vediamone alcuni:

* **Malware nel Kindle Swindle**: Questo ‘prodotto’ è chiamato  [Amazon Swindle](https://www.gnu.org/philosophy/why-call-it-the-swindle.html) ( gioco di parole sull'assonanza tra "Kindle" e "Swindle", che vuol dire truffa).

Il Kindle-Swindle di Amazon ha una backdoor che è stata usata per [cancellare libri a distanza](http://pogue.blogs.nytimes.com/2009/07/17/some-e-books-are-more-equal-than-others/).

* **Malware in Echo**: Amazon Echo sembra avere una backdoor universale dato che [installa automaticamente gli "aggiornamenti"](https://en.wikipedia.org/wiki/Amazon_Echo#Software_updates).
* **Malware in Amazon Fire Stick**: Un **malware Android**ha iniziato ad infettare **Amazon Fire Stick**, la piccola chiavetta media player di casa Amazon da qualche mese [disponibile anche in Italia](https://www.hdblog.it/2017/11/07/Amazon-Fire-TV-Stick-ufficiale-italia-prezzo/). Il malware - di tipo worm, ovvero in grado di autoreplicarsi senza la necessità di legarsi ad altri programmi eseguibili - non è stato specificamente progettato per colpire la Fire Stick, che però risulta vulnerabile a causa del sistema operativo basato su Android.

**VALUTAZIONE DEL RISCHIO**

Iniziamo ora a parlare di valutazione del rischio, in particolare di **risk assessment** che, come già detto, indica la valutazione del rischio, è volto a individuare e analizzare i rischi per capire quali siano le priorità di intervento e produrre poi azioni strategiche per contenerli o attenuarli.

È bene definire alcuni aspetti fondamentali (già citati) per la valutazione del rischio:

* **Contesto**: azienda esposta al rischio
* **Asset (a):** valore dei beni su cui la minaccia impatta
* **Minaccia (m):** potenziale causa di un danno all’organizzazione e la sua **probabilità di accadimento p(m)**
* **Vulnerabilità (v):** componenti di un sistema privi di misure di sicurezza
* **Controlli (c):** misura preventiva o di recupero che modifica il rischio

Un metodo valido di valutazione del rischio deve avere le seguenti caratteristiche:

• **completezza:** devono essere considerati, al giusto livello di sintesi, tutti gli asset, tutte le minacce e tutte le vulnerabilità;  
• **ripetibilità**: valutazioni condotte nello stesso contesto e nelle stesse condizioni devono dare gli stessi risultati;  
• **comparabilità:** valutazioni condotte in tempi diversi nello stesso contesto devono permettere di comprendere se il rischio è cambiato e come; deve essere anche nel tempo;  
• **coerenza:** a fronte di valori di asset, minacce e vulnerabilità più elevati di altri, il livello di rischio deve essere più elevato.

**ASSET**

Con il termine asset(bene) si fa riferimento a qualsiasi cosa che abbia valore per l’organizzazione come risorse, software, informazioni. In particolar modo possiamo identificare alcune categorie:

* **Informazioni**: Fanno parte di questa categoria i database e tutti i dati degli utenti registrati sulla piattaforma, ma anche i dati dei venditori e delle loro organizzazioni: quindi si parla di informazioni per la gestione commerciale e operativa dei fornitori; informazioni sul personale dell’organizzazione; informazioni sui prodotti presenti in magazzino e sulla programmazione della produzione; informazioni sulla creazione e resoconti delle verifiche dei prodotti realizzati.
* **Hardware e software**: Fanno parte di questa categoria i servizi informatici di supporto con relativi archivi informatici: i computer del personale e i server per la gestione delle e-mail e la condivisione del file; il sistema informatico di controllo del magazzino e della produzione con relativo archivio informatico che è accessibile dal personale interno; il servizio CRM**2** (Custom relation Management con relativo archivio informatico); gli impianti elettrici; gli archivi cartacei.

**2:** In economia aziendale il concetto di customer relationship management (CRM) o gestione delle relazioni con i clienti è legato al concetto di fidelizzazione dei clienti. In un'impresa "*market-oriented*" il mercato non è più rappresentato solo dal cliente, ma dall'ambiente circostante, con il quale l'impresa deve stabilire relazioni durevoli di breve e lungo periodo, tenendo conto dei valori dell'individuo/cliente, della società e dell'ambiente. Quindi l'attenzione verso il cliente è cruciale e determinante. Queste informazioni sono normalmente classificati riservati al marketing management che deve pianificare e implementare opportune strategie per gestire una risorsa così importante.

**MINACCE**

Parliamo di minaccia ogni volta che si verifica un incidete relativo alla sicurezza delle informazioni relative a uno o più eventi inattesi che hanno un’alta probabilità di compromettere le attività e di minacciare la sicurezza delle informazioni.

Quindi in breve, la minaccia è una causa potenziale di un incidente, che può comportare danni ad un sistema o all’organizzazione: le minacce non riguardano l’intera organizzazione ma aree specifiche.

Gli attori delle minacce potrebbero far parte del personale interno dell’organizzazione, tra cui responsabili di funzione, ma anche clienti e fornitori. Proprio per questo a ciascuno di loro viene comunicato solo quanto necessario affinché possa contribuire alle diverse fasi.

L’analisi di questo rischio richiede di identificare e valutare tutte le minacce relative alla sicurezza delle informazioni, non sono quelle informatiche o quelle più significative.

**TABELLA MINACCIA-ASSET-PROBABILITA’**

Le minacce che prendo in considerazione in questo caso di studio sono:

1. **Malware** 🡪 “software malevolo”, termine che descrive un programma/codice dannoso che mette a rischio un sistema. I malware sono molto invasivi e ostili, agiscono assumendo il controllo totale o parziale dei computer aziendali, del server dell’azienda e del sito web dedicato.
2. **DDOS** 🡪 “Distribuited denial-of-service” consiste nell’inviare intenzionalmente grandi quantità di dati a un obiettivo da diverse fonti per impedire a un utente, gruppi di utenti e all’organizzazione di accedere a una risorsa di rete.

Un attacco Distributed Denial of Service di ben 2,3 terabit al secondo è il mastodontico bombardamento di traffico da cui ha dovuto difendersi Amazon Web Services durante il mese di febbraio 2020. E' la stessa Amazon a divulgare l'accaduto all'interno del suo [Q1 2020 Threat Report](https://aws-shield-tlr.s3.amazonaws.com/2020-Q1_AWS_Shield_TLR.pdf), evidenziando il più massiccio attacco DDoS mai registrato fino ad ora.

1. **Problemi tecnici 🡪 “Errori di manutenzione hardware e software di base”,** Consiste nel NON funzionamento dell’hardware e software dell’organizzazione, dovuto a un errore o ad una mancata manutenzione. Un guasto all’impianto di produzione.
2. **Data Breach** 🡪 è la violazione dei dati personali di utenti, personale e fornitori; una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, perdita, modifica, divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o trattati.

L'ultima violazione dei dati che ha coinvolto Amazon si è verificata nell'ottobre 2020, quando un dipendente scontento di Amazon ha divulgato i dati dei clienti a terzi per la seconda volta quell'anno.

1. **Incendio** 🡪 Lo scoppio di un incendio colpisce l’hardware dell’organizzazione

L’ultimo evento di cui si ha notizia risale a Gennaio 2021 dove a Milano è divampato un incendio in un magazzino Amazon.

|  |  |  |
| --- | --- | --- |
| **Minaccia** | **Asset** | **Probabilità** |
| Malware | Computer aziendali, server e sito web | Alta |
| DDOS | Erogazione dei servizi online | Alta |
| Problemi tecnici | manutenzione hardware e software di base | Media |
| Data Breach | Dati personali di utenti, personale e fornitori | Media |
| Incendio | Hardware dell’organizzazione | Bassa |

*Tabella da Fogli di calcolo “Minacce-Asset-probabilità”*

**IMPATTO DELLE MINACCE SUI PARAMETRI RID**

Queste minacce si applicano sulle singole componenti del RID e hanno un diverso impatto sui **parametri RID**:

* **Riservatezza (Confidentiality)**: le informazioni non devono essere divulgate ne entrare in possesso a terzi non autorizzati, devono quindi essere accessibili unicamente a individui, entità o processi autorizzati.
* **Integrità (Integrity)**: la capacità di mantenere la veridicità dei dati e delle risorse e garantire che non siano in alcun modo modificate o cancellate;
* **Disponibilità (Availability)**: La possibilità per i soggetti autorizzati di poter accedere e utilizzare le risorse di cui hanno bisogno per un tempo stabilito ed in modo ininterrotto.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **m** | **Minaccia** | **R** | **I** | **D** |
| 1 | Malware | x | x | x |
| 2 | DDOS |  |  | x |
| 3 | Problemi tecnici |  | x | x |
| 4 | Data Breach | x |  |  |
| 5 | Incendio |  | x | x |

*Tabella da Fogli di calcolo “Minacce”*

Come riportato nella ISO/IEC 27001, c’è bisogno della valutazione delle conseguenze dei rischi che si dovessero concretizzare. La valutazione delle conseguenze è equiparata alla valutazione degli **impatti** **i(m,a)** di ciascuna **minaccia m** su ogni **asset a**. In pratica, si può determinare inizialmente il valore dell’**asset I(a)** in termini di riservatezza, integrità e disponibilità (parametri RID), utilizzando la formula:

**i(a) = (I-ris(a), I-int(a), I-dis(s))**

A questo punto, una volta identificate le probabilità e gli impatti sui parametri RID, posso calcolare il livello di rischio: questa misura è espressa come la combinazione delle conseguenze di una minaccia con la **verosimiglianza v**, cioè la probabilità che quella minaccia si manifesti. Più è elevato l’impatto, più alto sarà percepito il rischio. Il rischio dipende dalla minaccia; il rischio intrinseco è indipendente dalla gravità, per cui:

**r(m,a,v) ∝ p(m) ⋅ i(m,a)**

*Quindi riassumiamo così il significato della formula:*

Il rischio della minaccia sull’asset è direttamente proporzionale alla probabilità della minaccia per l’impatto che tale minaccia ha sull’asset.

**RISCHIO INTRINSECO QUANTITATIVO**

*Definizione analisi quantitativa*: Si definisce quantitativa una [ricerca di mercato](https://www.qualtrics.com/it/experience-management/ricerca/ricerca-di-mercato-una-guida/) costruita in modo da ottenere dati statisticamente rappresentativi di un mercato o di un suo segmento. Tale indagine proviene dal campo di ricerca sociale empirica e, pertanto, prevede la raccolta di dati numerici. Tali dati sono poi analizzati ed elaborati statisticamente per testare ipotesi o gettare luce su nuovi argomenti.

*Più in generale:* Con il metodo quantitativo determiniamo un rischio preciso misurato, normalmente in termini economici es. moneta.

L’analisi quantitativa analizza in particolare gli accadimenti del rischio e ne misura gli effetti sull’organizzazione. Questa analisi viene effettuata in un primo momento senza tener conto dei controlli di sicurezza, analizzando il rischio intrinseco.

Il **rischio intrinseco RI(m,a)** è dato dalla somma dei rischi scomposti RI-Ris(m,a), RI-Int(m,a) e RI-Dis(m,a), ottenuti così:

**RI-Ris(m,a) = p(m) \* Ris(m) \* Ris(a)**

**RI-Int(m,a) = p(m) \* Int(m) \* Int(a)**

**RI-Dis(m,a) = p(m) \* Dis(m) \* Dis(a)**

**RI(m,a) = RI-Ris(m,a) + RI-Int(m,a) + Ri-Dis(m,a)**

Immagine che contiene tavolo

Descrizione generata automaticamente

*Tabella da Fogli di calcolo “Rischio Intrinseco”*

Nel rischio intrinseco senza controlli, la minaccia più probabile è il malware con un impatto molto alto (sulla quale andrò ad intervenire in questo caso di studio ), quella meno probabile invece, è l’incendio. I grafici a dispersione risultanti mostrano visivamente questa affermazione:

**CONTROLLI DI SICUREZZA**

Sulla base del livello di rischio vanno individuati ed effettuati i controlli di sicurezza.

A ciascuna minaccia abbiamo associato un rischio intrinseco, si può quindi determinare come i controlli devono essere realizzati in modo proporzionale al rischio intrinseco.

Un rischio può essere controllato con misure preventive, di recupero e di rilevazione.

Il **rischio totale R(m,a,c**) è dato dalla somma di R-Ris(m,a,c), R-Int(m,a,c) e R-Dis(m,a,c) ottenuti in questo modo:

**R-Ris(m,a,c) = p(m) \* Ris(m) \* Ris(a,c)**

**R-Int(m,a,c) = p(m) \* Int(m) \* Int(a,c)**

**RI-Dis(m,a,c) = p(m) \* Dis(m) \* Dis(a,c)**

**RI(m,a,c) = RI-Ris(m,a,c) + R-Int(m,a,c) + R-Dis(m,a,c)**

Le metodologie di tipo quantitativo prevedono di calcolare di quanto ridurre la probabilità della minaccia o gli impatti grazie alla presenza di controlli di sicurezza.

I *controlli* *di sicurezza* che per ogni minaccia prendo in considerazione per questo caso di studio, sono:

1. **Malware** 🡪 Installazione di antivirus; formazione del personale; eseguire il backup giornaliero dei file e dei dati.
2. **DDOS** 🡪 Attivazione del Firewall sulla rete dell'organizzazione.
3. **Problemi tecnici** 🡪 Manutenzione periodica dei sistemi hardware e controlli/aggiornamenti periodici dei sistemi software; formazione del personale.
4. **Data Breach** 🡪 Utilizzo e/o installazione di sistemi per il rilevamento degli accessi e dei dispositivi connessi.
5. **Incendio** 🡪 Controllo e manutenzione periodica di estintori e sistemi di rilevamento del fumo.

Immagine che contiene tavolo

Descrizione generata automaticamente

*Tabella da Fogli di calcolo “Livello di rischio quantitativo”*

I controlli di sicurezza escludono/riducono la vulnerabilità; quindi possono modificare la probabilità di riuscita di una minaccia o gli impatti conseguenti.

Non è detto che tutti i controlli debbano impattare sulla probabilità.

**RAPPRESENTAZIONE DEL RISCHIO TOTALE**

Dopo aver applicato i controlli di sicurezza, la probabilità di accadimento del rischio malware (come verificato, la più elevata) si è attenuata.

Quindi questo sta ad indicare che il controllo di sicurezza è ideale, infatti applicandolo la probabilità di accadimento della minaccia è diminuita.

I grafici a dispersione risultanti mostrano visivamente questa affermazione:

**CONFRONTO TRA RI(m,a,) E R(m,a,c)**

Osserviamo i grafici ottenuti del Rischio intrinseco RI(m,a) e del Rischio totale R(m,a,c) e metto a confronto i valori ottenuti:

Riporto i *valori totali* ottenuti:

* RI(m,a) = 34,35
* R(m,a,c) = 10,11

Riporto anche i valori totali ottenuti per la minaccia *malware*:

* RI(m,a) = 16,2
* R(m,a,c) = 4,5

Riporto anche i valori totali ottenuti per la minaccia *DDOS*:

* RI(m,a) = 6,3
* R(m,a,c) = 2,1

Riporto anche i valori totali ottenuti per la minaccia *Problemi tecnici*:

* RI(m,a) = 7,2
* R(m,a,c) = 1

Riporto anche i valori totali ottenuti per la minaccia *Data Breach*:

* RI(m,a) = 3,6
* R(m,a,c) = 1,6

Riporto anche i valori totali ottenuti per la minaccia *Incendio*:

* RI(m,a) = 1,05
* R(m,a,c) = 0,91

Quindi posso affermare che applicando i controlli di sicurezza la probabilità di accadimento delle minacce è diminuita, in particolar modo cito la minaccia malware, minaccia con la maggior probabilità di accadimento si è attenuata.

Il calcolo dell’attenuazione del rischio mostrato in tabella quindi, mi dice di quanto la singola minaccia si è attenuata dopo aver applicato i controlli.

**ATTENUAZIONE DEL RISCHIO**

Arrivati a questo punto, una volta aver applicato i controlli, è possibile calcolare l’**attenuazione del rischio R(m,a,c)** per ogni componente RID su ogni minaccia come somma delle differenze del rischio intrinseco meno il rischio calcolato utilizzando i controlli.

Immagine che contiene tavolo

Descrizione generata automaticamente

*Tabella da Fogli di calcolo “Attenuazione del rischio”*

Dai valori risultanti notiamo come il guadagno più grande che abbiamo avuto è di 11,7 sulla minaccia malware.

Questo livello va continuamente valutato per vedere se in altri momenti i valori sono cambiati: se ad esempio la differenza è scesa significa che l’impatto è aumentato e io devo capire dove è aumentato, su che parametro.

**ANALISI QUALITATIVA**

*Definizione:* Con ricerca qualitativa si descrive un metodo scientifico che mira a raccogliere e valutare dati non-standard. I dati qualitativi forniscono informazioni che, invece di misurare un argomento, lo descrivono: ovvero tutte quelle informazioni relative alle motivazioni e agli atteggiamenti delle persone in forma di opinioni e punti di vista.

*Più in generale:* Con il metodo qualitativo determiniamo un livello di rischio indicato normalmente da un indice (1,2, 3 ecc.)

Adesso quello che andiamo a fare è assegnare un valore **g(v),** cioè il rischio che dipende dalle **vulnerabilità v** e dalla loro **gravità g**, in base a una scala di valori basata sull’adeguatezza dei controlli seguendo queste indicazioni:

**3** - Controlli di sicurezza *inadeguati* o *non attuati* (ossia completamente non conformi), se non sporadicamente; oppure Rilevate gravi vulnerabilità.

**2** - Controlli di sicurezza *non completamente adeguati* oppure attuati ma non in modo sistematico o con delle non conformità; oppure Rilevate lievi vulnerabilità.

**1** - Controlli di sicurezza *adeguati* ed attuati in modo sistematico e conforme; oppure Non rilevate vulnerabilità.

Per questo calcolo del livello di rischio, è sufficiente moltiplicare il valore del rischio intrinseco per il valore della vulnerabilità. La formula utilizzata è la seguente:

**r(m, a, v) = max[p(m) ⋅ ris(m) ⋅ ris(a), p(m) ⋅ int(m) ⋅ int(a), p(m) ⋅ dis(m) ⋅ dis(a)] ⋅ g(v)**

Prima di applicare la formula, come è possibile osservare in tabella, quello che faccio è assegnare un valore g(v) in questo modo:

* Malware 🡪 2
* DDOS 🡪 2

*Si moltiplica il valore massimo trovato per la gravità*

* Problemi tecnici 🡪 1
* Data Breach 🡪 2
* Incendio 🡪 3

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Minaccia** | **Minaccia descr.** | **R** | **I** | **D** | **g(v)** | **RI-ris(m,a)** | **RI-int(m,a)** | **RI-dis(m,a)** | **MAX** | **Ris(m,a,v)** |
| 1 | Malware | x | x | x | 2 | 4,5 | 6,3 | 5,4 | 4,5 | 9 |
| 2 | DDOS |  |  | x | 2 | 0 | 0 | 6,3 | 6,3 | 12,6 |
| 3 | Problemi Tecnici |  | x | x | 1 | 0 | 2,4 | 4,8 | 5,4 | 5,4 |
| 4 | Data Breach | x |  |  | 2 | 3,6 | 0 | 0 | 6,3 | 12,6 |
| 5 | Incendio |  | x | x | 3 | 0 | 0,56 | 0,49 | 4,8 | 14,4 |
|  |  |  |  |  |  |  |  | **Totale** | 27,3 | 54 |

*Tabella da Fogli di calcolo “Rischio qualitativo”*

**[***NOTA*: In giallo sono evidenziati i valori che scelgo come MAX, ovvero i 5 valori più grandi calcolati; perché non facciamo più la somma ma applichiamo il livello massimo.**]**

**NORMALIZZAZIONE DEL RISCHIO**

Un’altra metodologia qualitativa è la normalizzazione del rischio, attraverso la quale è possibile assegnare dei livelli di rischio intrinseco rispetto a tabelle normalizzate al fine di riportare i valori del rischio ad una scala predefinita, per riportare i valori del rischio ad una scala predefinita [p(m),i(a)] cioè in funzione della probabilità p(x) e della conseguenza i(a) :



La normalizzazione è quel processo che ci permette di passare dal rischio quantitativo al rischio qualitativo, e non il contrario.

Questa procedura è necessaria poiché qualche volta non è possibile stimare la probabilità con precisione.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Minaccia** | **Minaccia descr.** | **R** | **I** | **D** | **p(m)** | **Ris(m)** | **Int(m)** | **Dis(m)** | **Ris(a)** | **Int(a)** | **Dis(a)** | **RI-ris(m,a)** | **RI-int(m,a)** | **RI-dis(m,a)** | **RI(m,a)** |
| 1 | Malware | x | x | x | 0,9 | 0 | 1 | 1 | 5 | 7 | 6 | 0 | 6,3 | 5,4 | 11,7 |
| 2 | DDOS |  |  | x | 0,7 | 0 | 0 | 1 | 0 | 0 | 9 | 0 | 0 | 6,3 | 6,3 |
| 3 | Problemi Tecnici |  | x | x | 0,6 | 0 | 1 | 1 | 0 | 4 | 8 | 0 | 2,4 | 4,8 | 7,2 |
| 4 | Data Breach | x |  |  | 0,4 | 1 | 0 | 0 | 9 | 0 | 0 | 3,6 | 0 | 0 | 3,6 |
| 5 | Incendio |  | x | x | 0,07 | 0 | 1 | 1 | 0 | 8 | 7 | 0 | 0,56 | 0,49 | 1,05 |

Immagine che contiene tavolo

Descrizione generata automaticamente

*Tabelle da Fogli di calcolo “Normalizzazione”*

L’analisi che posso fare è trasversale: orizzontale o verticale.

In questo caso quello che vado a fare è un’analisi orizzontale perché in questo modo riesco a capire sulla singola minaccia dell’asset cosa accade.

A me non interessano più i numeri iniziali, ma i livelli.

Abbandoniamo i numeri e andiamo sulla formula qualitativa che è data dal massimo livello di rischio che abbiamo.

Il mio punto di partenza sono sempre le probabilità.

Le probabilità e gli impatti vengono divisi in aree e le minacce su ogni componente RID vengono mappate nelle aree create.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Classificazione** | | **RID** |  |  |  |
|  |  |  |  |  |  |
| probabilità p(m) | alta | **0,66-1,00** | **DDOS RI** | **Malware RID** | **DDOS D** |
| media | **0,34-0,65** | **Data Breach ID Problemi tecbnici R** | **Problemi tecnici I** | **Data Breach R Problemi tecnici D** |
| bassa | **0,00-0,33** | **Incendio R** | **Incendio D** | **Incendio I** |
|  |  |  | **0-3** | **4-7** | **8-10** |
|  |  |  | conseguenza impatto i(a) | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Classificazione** | | **Totale** |  |  |  |
|  |  |  |  |  |  |
| probabilità p(m) | alta | **0,66-1,00** |  | **DDOS** | **Malware** |
| media | **0,34-0,65** |  | **Data Breach problmei tecnici** |  |
| bassa | **0,00-0,33** |  | **Incendio** |  |
|  |  |  | **bassa** | **media** | **alta** |
|  |  |  | conseguenza impatto i(a) | | |

*Tabella da Fogli di calcolo “Normalizzazione”*

È così possibile definire l’opzione di trattamento più appropriata alla gestione della minaccia:

|  |  |
| --- | --- |
| prevenzione | Prevenzione e  recupero |
| accettabile | Recupero |

**TEST STATISTICI**

Un test statistico è una procedura che consente di verificare con un elevato grado di fiducia una nostra ipotesi iniziale *H*0, che si chiama anche *ipotesi di lavoro* o *ipotesi nulla*, inerente a un fenomeno che stiamo studiando. Il test essenzialmente è una procedura di calcolo che si basa sull’analisi dei dati numerici che abbiamo a disposizione, dati che sono interpretati come valori osservati di una certa variabile aleatoria. Tale procedura di calcolo si conclude fornendo un numero, un *consuntivo*, che permette di confermare oppure di respingere l’ipotesi di lavoro, in favore di un’altra ipotesi iniziale *H*1, detta *ipotesi alternativa*.

Viene usata una misura di sintesi probabilistica per trarre conclusioni sull’evidenza contro l’ipotesi nulla in un test a partire dai dati. Si dice p-value il più piccolo valore del livello di significatività α per cui i dati campionari consentono di rifiutare H0. Se il p-value è troppo piccolo si rifiuta l’ipotesi H0, altrimenti la si accetta.

La variabile casuale, detta anche aleatoria o stocastica, è una variabile che può assumere valori diversi dipendentemente a qualche fenomeno aleatorio (es: lancio del dato, estrazioni, probabilità che si verifichi un incendio ecc).

Il termine aleatorio esprime il concetto di rischio calcolato.

I test statistici effettuati di seguito, sono fatti con variabili casuali discrete, cioè abbiamo dei numeri di eventi deterministici (x=0,1,2 ecc..)

**VARIABILI CASUALI-BINOMIALI**

La binomiale è ottima come variabile casuale e gestisce eventi che possono essere anche molto grandi.

Nell’ipotesi di **n** prove ripetute di eventi con probabilità di evento favorevole **π e** probabilità sfavorevole **1- π:**

* *Media* µ = E(X) = n π
* *Varianza* 𝜎2= n π (1-π)

Nelle prove ripetute, se delle n prove ipotizziamo k eventi favorevoli:

In questo caso di studio, la Binomiale viene usata per la ***minaccia di Data Breach***, con probabilità **π=0,5.** Posso quindi calcolare la probabilità complementare **1- π=0,5.**

*Dati:*

Numero di prove ripetute n = 10

Eventi favorevoli k = 1…10

Probabilità evento favorevole (minacce) π = 0,5

Probabilità complementare (ev. sfavorevole) 1- π = 0,5

Media µ = n π = 10\*0,5 = 5

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **X (k)** | **n!** | **k!(n-k)!** | **n su k** | **π^k** | **(1-π)^(n-k)** | **P(X)** | **Cum P(X)** |
| 0 | 3628800 | 3628800 | 1 | 1,00000 | 0,00098 | 0,0009766 | 0,0009766 |
| 1 | 3628800 | 362880 | 10 | 0,50000 | 0,00195 | 0,0097656 | 0,0107422 |
| 2 | 3628800 | 80640 | 45 | 0,25000 | 0,00391 | 0,0439453 | 0,0546875 |
| 3 | 3628800 | 30240 | 120 | 0,12500 | 0,00781 | 0,1171875 | 0,0009766 |
| 4 | 3628800 | 17280 | 210 | 0,06250 | 0,01563 | 0,2050781 | 0,3769531 |
| 5 | 3628800 | 14400 | 252 | 0,03125 | 0,03125 | 0,2460938 | 0,6230469 |
| 6 | 3628800 | 17280 | 210 | 0,01563 | 0,06250 | 0,2050781 | 0,8281250 |
| 7 | 3628800 | 30240 | 120 | 0,00781 | 0,12500 | 0,1171875 | 0,9453125 |
| 8 | 3628800 | 80640 | 45 | 0,00391 | 0,25000 | 0,0439453 | 0,9892578 |
| 9 | 3628800 | 362880 | 10 | 0,00195 | 0,50000 | 0,0097656 | 0,9990234 |
| 10 | 3628800 | 3628800 | 1 | 0,00098 | 1,00000 | 0,0009766 | 1,0000000 |

*Tabella da Fogli di calcolo “Binomiale-data breach”*

Osserviamo i grafici risultanti relativi alla P(X) e alla funzione di ripartizione di probabilità (cumulata):

Più la curva è alta, meno è variabile.

Mi interessa molto la cumulata perché parlando di analisi del rischio, a me interessa sapere a priori qual è il livello più alto, con probabilità maggiore di eventi che io posso subire.

**PROBABILITA’ COMPOSTA DI DATA BREACH**

A questo evento di Data Breach supponiamo di aggiungere una ***probabilità composta***.

Quello che accade simultaneamente quindi è che:

* Avviene un data breach;
* I sistemi per il rilevamento degli accessi e dei dispositivi connessi non funzionano.

Alla probabilità dell’evento favorevole di avvenimento del Data Braech π = 0,5 devo correlare la **variabile casuale di non funzionamento dei sistemi per il rilevamento degli accessi e dei dispositivi connessi** **π’=0,05** (ovvero c’è un 5% di probabilità che il sistema di rilevamento non funzioni).

La probabilità totale è data da:

**Ptot(Data Braech + Malfunzionamento sistema)** = **π\* π’**= 0,5\*0,05 = 0,025

Rifaccio quindi i calcoli con questi *dati*:

Numero di prove ripetute n = 10

Eventi favorevoli k = 1…10

Probabilità evento favorevole π = 0,025

Probabilità complementare (ev. sfavorevole) 1- π = 0,975

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **X (k)** | **n!** | **k!(n-k)!** | **n su k** | **π^k** | **(1-π)^(n-k)** | **P(X)** | **Cum P(X)** |
| 0 | 3628800 | 3628800 | 1 | 1,0000000 | 0,77633 | 0,7763296 | 0,7763296 |
| 1 | 3628800 | 362880 | 10 | 0,0250000 | 0,79624 | 0,1990589 | 0,9753885 |
| 2 | 3628800 | 80640 | 45 | 0,0006250 | 0,81665 | 0,0229683 | 0,9983568 |
| 3 | 3628800 | 30240 | 120 | 0,0000156 | 0,83759 | 0,0015705 | 0,9999273 |
| 4 | 3628800 | 17280 | 210 | 0,0000004 | 0,85907 | 0,0000705 | 0,9999978 |
| 5 | 3628800 | 14400 | 252 | 0,0000000 | 0,88110 | 0,0000022 | 1,0000000 |
| 6 | 3628800 | 17280 | 210 | 0,0000000 | 0,90369 | 0,0000000 | 1,0000000 |
| 7 | 3628800 | 30240 | 120 | 0,0000000 | 0,92686 | 0,0000000 | 1,0000000 |
| 8 | 3628800 | 80640 | 45 | 0,0000000 | 0,95063 | 0,0000000 | 1,0000000 |
| 9 | 3628800 | 362880 | 10 | 0,0000000 | 0,97500 | 0,0000000 | 1,0000000 |
| 10 | 3628800 | 3628800 | 1 | 0,0000000 | 1,00000 | 0,0000000 | 1,0000000 |

*Tabella da Fogli di calcolo “Probabilità composta – D.B.”*

Questa probabilità dell’evento composto è molto bassa, vicino all’1. In questo caso posso non considerare questa situazione perché è molto bassa.

Decido quindi di mantenere solo l’evento di Data Breach.

**VARIABILI CASUALI – POISSON**

La distribuzione di Poisson, anche chiamata distribuzione degli eventi rari, è una approssimazione della distribuzione binomiale, definita per valori interi non negativi.

Possiamo dire quindi che la distribuzione di Poisson valorizza eventi rari che hanno una media un po’ più bassa.

La variabile casuale quindi, caratterizza bene eventi che si manifestano con una distribuzione media di probabilità prossima allo zero ed una asimmetria destra che denota una bassissima probabilità che gli eventi si verifichino più volte.

Immagine che contiene testo

Descrizione generata automaticamentePossiamo quini calcolare la **P(X)** così:

Dove:

* e = numero di Neplero = 2,718
* µ = λ Valore medio
* 𝜎2 = λ Varianza *Nella Poisson la media e la varianza coincidono.*
* 𝜎 = √ λ

In questo caso di studio, la variabile di Poisson viene usata per la ***minaccia di incendio***, con probabilità **π=0,07** (essendo un evento raro la probailità è molto bassa).

Posso quindi calcolare la probabilità complementare **1- π=0,93.**

*Dati:*

Numero di giorni n = 10

Eventi favorevoli k = 1…10

Probabilità evento favorevole π = 0,07

Probabilità complementare (ev. sfavorevole) 1- π = 0,93

Media µ= 𝜎2 = λ= n π = 0,7

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **X** | **e^(-λ)** | **λ^x** | **x!** | **P(X)=e^(-λ)\*(λ^X/X!)** | **Cum P(X)** | **P value** |  | **X** | **P value** |  |
| 0 | 0,496621 | 1,0000000 | 1 | 0,496621347 | 0,483982307 | 0,516017693 |  | 0 | >50% |  |
| 1 | 0,496621 | 0,7000000 | 1 | 0,347634943 | 0,848270065 | 0,151729935 |  | 1 | <50% |  |
| 2 | 0,496621 | 0,4900000 | 2 | 0,121672230 | 0,971657854 | 0,028342146 |  | 2 | <5% |  |
| 3 | 0,496621 | 0,3430000 | 6 | 0,028390187 | 0,996423862 | 0,003576138 |  | 3 | <1% |  |
| 4 | 0,496621 | 0,2401000 | 24 | 0,004968283 | 0,999686051 | 0,000313949 |  | 4 | <0,1% |  |
| 5 | 0,496621 | 0,1680700 | 120 | 0,000695560 | 0,999980701 | 0,000019299 |  | 5 | <0,01% |  |
| 6 | 0,496621 | 0,1176490 | 720 | 0,000081149 | 0,999999182 | 0,000000818 |  | 6 | <0,001% |  |
| 7 | 0,496621 | 0,0823543 | 5040 | 0,000008115 | 0,999999977 | 0,000000023 |  | 7 | <0,001% |  |
| 8 | 0,496621 | 0,0576480 | 40320 | 0,000000710 | 1,000000000 | 0,000000000 |  | 8 | <0,001% |  |
| 9 | 0,496621 | 0,0403536 | 362880 | 0,000000055 | 1,000000000 | 0,000000000 |  | 9 | <0,001% |  |
| 10 | 0,496621 | 0,0282475 | 3628800 | 0,000000004 | 1,000000000 | 0,000000000 |  | 10 | <0,001% |  |

*Tabella da Fogli di calcolo “Poisson - Incendio”*

* Il p value è il valore inverso della cumulata (dato da 1 – il valore della cumulata).

È la stima dell’errore. Più è basso meglio è la stima che sto facendo.

Se considero pochi eventi, ad esempio i primi 2 notiamo che hanno un colore rosso intenso, cioè sono molto lontani dalla certezza.

* Se voglio una probabilità a cui stare sicuro, fisso i livelli: 90%, 95%, 99% (sono i livelli di confidenza più utilizzati).

Questo significa che se voglio un sistema che sia sicuro al 95%, gli eventi che posso gestire sono gli eventi 0 e 1.

Se invece voglio un sistema che sia sicuro al 99% dovrò gestire gli eventi almeno fino a 3 (devo poi gestire i resti).

Nel caso della binomiale, invece, per avere un sistema che sia sicuro al 99% dovrò gestire gli eventi almeno fino a 9.

Osserviamo i grafici risultanti relativi alla P(X) e alla funzione di ripartizione di probabilità (cumulata):

La Poisson rispetto alla binomiale si trova più vicino all’origine.

Le probabilità accumulate sono molto importanti. Diciamo che io voglio essere sicuro al 99%. Se ipotizzo che questo evento non si verifichi mai, la probabilità cumulata è 0,48; se ipotizzo che l’evento è avvenuto almeno una volta, quindi o zero o 1, vediamo come le probabilità si sommano, infatti siamo già a 0,84.

Ipotizziamo invece che P(X) deve essere almeno 2: P(X<=2) = 0,97 = 97%

Io però voglio arrivare al 99% minimo, quindi devo arrivare a x=3, quindi il valore soglia è 3.

Le variabili usate per i test statistici sono variabili casuali discrete. Se vogliamo utilizzare variabili casuali continue dobbiamo far riferimento a la normale (Gaussiana) che è una delle distribuzioni di probabilità più diffuse nei problemi pratici in quanto modella buona parte della distribuzione di probabilità in eventi reali.

**CONCLUSIONI**

Concludendo posso dire che l’azienda Amazon.com, essendo una grande azienda sviluppata in più campi, è esposta a molti rischi. Le minacce analizzate in questo caso di studio sono solo 5, ma effettivamente le minacce che colpiscono questa organizzazione sono molte di più e sono appartenenti alle più svariate categorie. Ad esempio per quanto riguarda la categoria dei danni fisici ho scelto di analizzare solamente la minaccia ‘incendio’, ma le minacce di questa categoria che potrebbero colpire l’azienda potrebbero essere anche: ‘allagamento’, ‘distruzione di strumentazione da parte di malintenzionati o per errore (disattenzione)’; e così via anche per le altre categorie.

Dopo aver analizzato le minacce attraverso prese in considerazione e le relative vulnerabilità riscontrate attraverso l’analisi del rischio intrinseco quantitativo, è emerso che la minaccia più probabile è quella di malware con un impatto molto alto, seguita dalle minaccia DDOS, problemi tecnici e Data Breach fino ad arrivare alla minaccia con minor probabilità, ovvero quella di incendio.

Fatta questa analisi, si è reso indispensabile avviare opzioni di recupero ma anche di prevenzione, attraverso la messa in atto di controlli adeguati.

Quindi, ad ogni minaccia sono stati associati dei controlli di sicurezza ed è emerso dopo l’analisi che questi escludono/riducono la vulnerabilità, quindi possono modificare la probabilità di riuscita di una minaccia o gli impatti conseguenti.

Ad esempio, notiamo come la minaccia malware (con la probabilità più alta di accadimento) si è attenuata. Il controllo di sicurezza che è stato applicato è ideale, la probabilità di accadimento è diminuita.

Si è passati quindi ad una analisi qualitativa del rischio, tenendo conto che il rischio dipende dalle vulnerabilità e dalla loro gravità in base a una scala di valori.

Un’altra metodologia di analisi qualitativa è la normalizzazione del rischio, cioè ho assegnato dei livelli di rischio intrinseco così da riportare i valori del rischio ad una scala predefinita. Questo è utile soprattutto quando non posso stimare la probabilità con precisione.

A questo punto posso effettuare i test statistici.

La variabile casuale binomiale viene usata per la minaccia di Data Braech.

Ho anche effettuato una prova di probabilità composta di Data Breach, formata da due eventi che accadono simultaneamente: Avviene un data breach e I sistemi per il rilevamento degli accessi e dei dispositivi connessi non funzionano. Cambia così la probabilità dell’evento favorevole e dopo i calcoli posso dire che la probabilità di questo evento composto è molto bassa, vicino all’1 e decido di non considerare questa situazione.

La variabile casuale di Poisson, invece, viene usata per la minaccia di incendio.