Università degli Studi di Bari 'Aldo Moro'
Dipartimento di Informatica
Corso di Laurea Magistrale in Sicurezza Informatica

CASO DI STUDIO
ORGANIZZAZIONE AZIENDALE
A.A. 2023/2024

Matteo Esposito

Introduzione

Ambiente

- Ambiente interno
  - Struttura Organizzativa
  - Risorse Umane
- Ambiente Esterno
  - Mercato e Concorrenza
  - Regolamentazione
  - Clienti e Fornitori

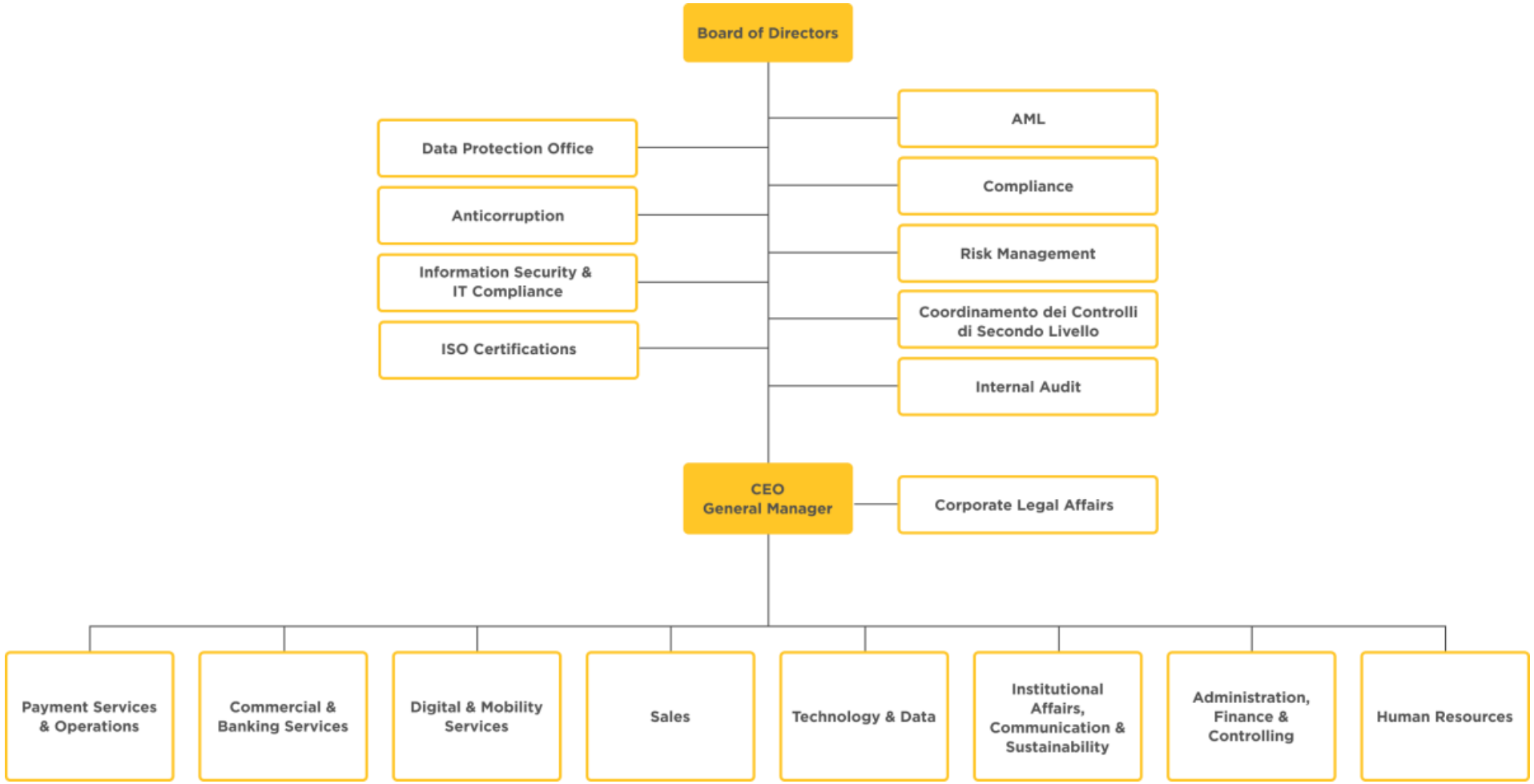
Attori

- Clienti
- Esercenti Affiliati
- Partner Aziendali
- Dipendenti e Collaboratori

Relazioni

- Collaborative
- Strategiche
- Con i consumatori
- Intra-organizzative

Stuttura Aziendale



Processi

Stutturabilità del processo

IMPATTO SULLE PERFORMANCE	ALTA	BASSA
DIRETTO	CORE: • Carte Prepagate, • Punti di Vendita • MooneyGO	NETWORK: • Alleanze strategiche • Collaborazioni
INDIRETTO	SUPPORT: • Risorse umane, • Conformità e Sicurezza, • Gestione Tecnologica	MANAGEMENT: • Pianificazione strategica • Monitoraggio e Controllo

Attacco

Attacco – Kill Chain

FASE	PROCESSO
RECONNAISSANCE	I criminali informatici raccolgono informazioni sulla loro vittima
WEAPONIZATION	L'attaccante scrive uno script in Python che cripta i file della vittima con AES-256, convertire lo script Python in un file .exe dall'aspetto credibile.
DELIVERY	L'email supera i filtri aziendali perché il mittente sembra legittimo e il messaggio è scritto in modo professionale. Potrebbe addirittura sembrare inviato dal reparto IT aziendale.
EXPLOITATION	L'ignaro dipendente scarica e avvia il file OfficeUpdate.exe, pensando di installare un aggiornamento.
INSTALLATION	Il ransomware viene installato e attivato.
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.
ACTIONS ON OBJECTIVES	Appare sul Desktop della vittima un file di testo contenente la richiesta di riscatto, per decrittografare il sistema.

Attacco – Delivery

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

Dipartimento di Informatica

Difesa - SOC

FASE	PROCESSO
RECONNAISSANCE	Monitorare attività sospette, come tentativi di raccolta informazioni o accessi non autorizzati ai sistemi.
WEAPONIZATION	Aggiornare le firme degli antivirus e configurare i sistemi di rilevamento per identificare e bloccare payload noti.
DELIVERY	Implementare filtri anti-phishing, monitorare il traffico e-mail e bloccare messaggi sospetti.
EXPLOITATION	Monitorare l'esecuzione di processi anomali e rilevare comportamenti sospetti sui sistemi degli utenti.
INSTALLATION	Rilevare e bloccare tentativi di installazione di software non autorizzato.
COMMAND AND CONTROL	Monitorare il traffico di rete per individuare comunicazioni sospette verso domini o indirizzi IP noti per attività malevole.
ACTIONS ON OBJECTIVES	Rilevare attività di cifratura anomala dei file e avvisare tempestivamente il CSIRT.

Difesa - CSIRT

FASE	PROCESSO
RECONNAISSANCE	Analizzare segnalazioni di attività anomale e preparare piani di risposta in caso di minacce identificate.
WEAPONIZATION	Analizzare nuovi malware, sviluppare indicatori di compromissione (IoC) e condividere informazioni sulle minacce emergenti.
DELIVERY	Rispondere a incidenti legati a e-mail malevole, analizzare campioni di phishing e aggiornare le difese.
EXPLOITATION	Indagare sugli incidenti, determinare l'entità dello sfruttamento e coordinare la risposta.
INSTALLATION	Analizzare il malware installato, identificare i vettori di infezione e rimuovere le minacce.
COMMAND AND CONTROL	Analizzare i pattern di comunicazione del malware e bloccare le connessioni ai server di comando e controllo.
ACTIONS ON OBJECTIVES	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.

Difesa – Support IT

FASE	PROCESSO
RECONNAISSANCE	Implementare misure preventive, come la protezione dei dati sensibili e la limitazione dell'esposizione pubblica delle informazioni aziendali.
WEAPONIZATION	Applicare patch di sicurezza ai software e limitare l'esecuzione di applicazioni non autorizzate.
DELIVERY	Educare i dipendenti sul riconoscimento delle email di phishing e implementare autenticazione a più fattori (MFA).
EXPLOITATION	Limitare i privilegi degli utenti, impedendo l'esecuzione di software non autorizzato.
INSTALLATION	Implementare controlli di integrità dei sistemi e monitorare le modifiche non autorizzate.
COMMAND AND CONTROL	Configurare firewall e sistemi di prevenzione delle intrusioni (IPS) per bloccare traffico verso destinazioni non autorizzate.
ACTIONS ON OBJECTIVES	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.

NIS 2

1. Analisi del rischio e misure di sicurezza
2. Notifica e gestione degli incidenti
3. Sicurezza della supply chain
4. Formazione e sensibilizzazione del personale
5. Controlli e audit periodici